FACULDADE ASCES

CURSO DE DIREITO

FERNANDA MIRELLE LOPES DE SOUSA

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO PENAL E FORMAS DE PREVENÇÃO

CARUARU

2015

FACULDADE ASCES

CURSO DE DIREITO

FERNANDA MIRELLE LOPES DE SOUSA

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO PENAL E FORMAS DE PREVENÇÃO

Trabalho de Conclusão de Curso, apresentado à Associação Caruaruense de Ensino Superior e Técnico, como requisito parcial para a obtenção do Grau de Bacharelado em Direito, sob orientação do Professor Arquimedes Melo.

CARUARU

2015

BANCA EXAMINADORA

Aprovada em: ____/___/____

_____

Presidente: Prof. Arquimedes Melo

_____

Primeiro Avaliador. Prof.

_____

Segundo Avaliador. Prof.

DEDICATÓRIA

Dedico este trabalho a meu namorado Maurílio, ao meu querido sobrinho Matheus Ramalho (a luz dos meus olhos) e a minha família.

AGRADECIMENTOS

Agradeço ao Prof. Arquimedes Melo, que além de orientador me ajudou para a conclusão deste trabalho.

Ao Prof. Adrielmo Moura pela sua atenção e também me forneceu material de pesquisa.

Ao meu grande amigo Jimy Davison que tantas vezes me ajudou, assim como também, aos demais docentes que me acompanharam durante a minha vida acadêmica.

RESUMO

O estudo do presente trabalho tem por objetivo procurar contribuir levando conhecimento aos cidadãos a respeitos do que é e de como agir caso sejam vítimas de um crime cibernético, e que se utilizando destes conhecimentos possam ter uma visão acerca de formas de prevenção, assim como também de combate a essa modalidade de crime, que apesar de recente, vem acometendo a sociedade de forma crescente. Expõe um breve relato histórico sobre o surgimento da rede mundial de computadores no Brasil e no mundo, faz menção a alguns delitos informáticos recorrentes na internet e faz a análise dos delitos citados, busca verificar as formas de ataques virtuais e as fragilidades do sistema e suas peculiaridades. Esclarece como os usuários que se utilizam da rede podem se proteger de possíveis ataques e lesões causadas pelos delinquentes virtuais. Apresenta de forma direta os assuntos relativos aos cibercrimes e a maneira com que os transgressores agem para lesar suas vítimas. Traz a forma como ele é cometido e os meios jurídicos existentes para reprimir e punir esta conduta. Comenta a importância do Marco civil da Internet e da Lei nº 12.737/12, popularmente conhecida por Lei Carolina Dieckmann, que alterou alguns dispositivos do Código Penal e demonstra a carência de leis penais para tipificar e penalizar os indivíduos que incidem nesta técnica criminosa.

PALAVRAS-CHAVE: Relato Histórico. Crimes cibernéticos. Fragilidades do sistema. Formas de combate. Legislação Específica.

ABSTRACT

The study of this work aims to contribute, providing knowledge to the citizens about what is, and what to do if they are victims of cybercrime, and using this knowledge may be to have a vision about how to prevent, as well as, how to combat this type of crime, which despite of recent, is affecting society increasingly. It exposes a brief historical account of the emergence of the World Wide Web in Brazil and worldwide, mentions some recurring computer crimes on the Internet and makes the analysis of the aforementioned offenses, it aims to verify the forms of cyber attacks and system weaknesses and their peculiarities. It explains how users can protect themselves from possible attacks and injuries caused by virtual criminals. It shows directly and succinctly the issues relating to cybercrime and the way the transgressors act to defraud their victims. It brings the way that it is made and the existing legal means to suppress and punish this conduct. Also, it comments the importance of the civilian Internet Code and Law 12.737 / 12, popularly known as Law Carolina Dieckmann, which amended some provisions of the Penal Code and demonstrates the lack of criminal laws to criminalize and penalize individuals who focus on this criminal technique.

KEY-WORDS: historical account. Cybercrimes. Weaknesses of the system. Forms of combat. Specific Legislation.

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

Cenas de crianças utilizando aparelhos eletrônicos até a alguns anos seria inimaginável, então o que se falar de mensagens sendo enviadas através de plataformas digitais a longas distâncias em fração de segundos, compras sendo feitas no clicar de um mouse ou conversas instantâneas com um amigo que está no outro lado do continente? Pois bem, esses avanços tecnológicos que têm nos trazido tantas comodidades também deu ensejo a problemas tão modernos quanto às utilidades desses recursos. Trata-se de crimes cibernéticos, espécie de delitos que estão se tornando cada vez mais comuns e vitimando jovens e adultos, se popularizando por conta da modernização que vem passando a sociedade.

A preocupação do homem em minimizar tarefas, agilizar as atividades rotineiras e o aumento da produtividade o levou a procurar métodos que o auxiliasse. Sua frequente curiosidade e entusiasmo por novidades, desde os tempos remotos até a atualidade, vem o impulsionando na inspiração de invenções, muitas de grande utilidade outras nem tanto, mas não menos importante, tem contribuído para a modernização da sociedade, infelizmente, junto com a praticidade oriunda da tecnologia cibernética veio à facilidade de se executar alguns crimes já tipificados no Ordenamento Jurídico, crimes estes, que têm na sua prática virtual maior facilidade e destreza, e como também a possibilidade de dar cumprimento a outros delitos que necessitam da tecnologia para que tenham êxito a sua execução e consumação.

Sendo assim, a consequência do avanço tecnológico foi à má utilização dos seus adventos e o que deveria ser utilizado para facilitar a vida do ser humano, como era o objetivo primordial, passou a servir para o seu prejuízo e tornou-se mais um problema com o qual as pessoas têm que aprender a lidar, que cresce à medida que se populariza e se banaliza, podendo agora ser praticado por qualquer pessoa e não apenas por quem tiver qualificado, sendo assim, a chegada de mais tecnologia aumenta as dificuldades de se encontrar o criminoso, ou seja, o desenvolvimento quase que descontrolado no que tange à área tecnológica, proporcionou o surgimento de alguns tipos delituosos virtuais difíceis de serem punidos, alastrando-se por todas as direções, tornando-se verdadeiras armadilhas aos que utilizam a rede mundial de computadores para realizar suas transações bancárias, efetuar compras, ou simplesmente checar sua caixa de e-mails.

O presente trabalho tem por objetivo difundir conhecimentos acerca dos cibercrimes, proporcionando à sociedade esclarecimentos e orientações acerca da forma de agir diante de

um crime cibernético, também como as formas de prevenção deste delito tão corriqueiro. Portanto, para atender a esse objetivo foi necessário descrever um breve histórico da evolução da internet e os avanços dos recursos tecnológicos, assim tentando esclarecer como surgiram os crimes cibernéticos e como a tecnologia poderá ser utilizada de forma indevida, analisar as técnicas de segurança da informação e as normas de segurança brasileira, buscou-se ainda demonstrar como os fatores técnico e humano tem papel fundamental na possibilidade do delito, buscando mostrar as principais fragilidades através de estatísticas e as formas de ataque mais cometidas. Verificou-se que a falta de conhecimento do cidadão comum em relação a uma tecnologia tão recente o tornou uma vitima em potencial, que muitas vezes contribuem, direta ou indiretamente com o delito quando, por exemplo, não tomam as devidas precauções ao utilizar-se do sistema informático.

Quanto ao autor foi constatado que este, diferentemente do que se imaginava, atualmente poderá ser qualquer pessoa, claro que a depender do tipo do delito, precisará ter um determinado conhecimento técnico, porém para muitos dos crimes cometidos atualmente, um domínio básico da tecnologia já será o suficiente.

Vale salientar que para o melhor entendimento deste tema se faz necessário uma análise de alguns crimes e sua forma de execução, contudo esclarecemos que este não é o principal objetivo deste trabalho e que improvável seria a descrição de todos os delitos que poderão ser praticados na forma virtual, tendo em vista a possibilidade de o avanço tecnológico trazer novos delitos virtuais.

Encerraremos mostrando as formas de prevenção e de combate, sendo este um ponto do trabalho de grande importância, pois é pretendido que traga contribuições à sociedade e que possa, através destas, vir a ser útil, proporcionando um melhor entendimento e consequentemente venha a influenciar na prevenção, assim como explanará os dispositivos presentes, atualmente, no nosso ordenamento jurídico que através destes existe a possibilidade da punição do agente e a proteção da sociedade.

Esses passos estão organizados em três capítulos. No primeiro capítulo apontará um levantamento histórico, fazendo uma análise do surgimento da informática no Brasil e no mundo, o surgimento das máquinas que antecederam os computadores e a criação do primeiro computador, a influencia da segunda guerra no desenvolvimento dos sistemas informáticos, e como essas máquinas se popularizaram com o passar dos anos, tornando-se indispensáveis. No mesmo capítulo será mostrado o surgimento da internet, sua popularização e mais uma vez a influência da segunda guerra, mostrará através de gráficos, os motivos de uso e as redes

sociais mais utilizadas, fechando o primeiro capítulo será mostrado a evolução histórica dos crimes cibernéticos.

No segundo capítulo, será abordados as fragilidades do sistema informático e como estes possibilitam a execução e consumação dos delitos, foi visto que as falhas técnicas do sistema tem papel fundamental para que os crimes venham a acontecer, porém o fator humano foi mostrado através de estatísticas, como sendo o maior responsável. Na sequência serão apontados alguns tipos de crimes que podem ser praticados no ambiente virtual, estando estes elencados em: crimes contra o patrimônio, crimes contra a honra e crimes contra a dignidade sexual, finalizando o segundo capítulo será indicado o papel da vítima do crime cibernético e como esta, muitas vezes tem papel fundamental na ocorrência do delito, contribuindo de forma direta ou indireta e o perfil do autor do crime cibernético, que diferentemente do que se pensa, a depender do crime, este pode ser cometido por qualquer um, ou seja, não sendo necessário possuir conhecimentos técnicos específicos.

No terceiro e último capítulo será estudado métodos de defesa, mostrando de forma clara as precauções que um cidadão comum poderá ter para evitar ser vítima de um crime virtual, em seguida as ações que deverão ser tomadas caso o delito já tenha se perpetrado. Para finalizar será estudado o Ordenamento Jurídico, o Marco Civil da internet e como esse versa sobre a Responsabilidade Civil dos provedores e dos usuários, e a Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, que incorporou alguns artigos ao Código Penal.

Este trabalho de pesquisa monográfica tem como público alvo o cidadão comum, indivíduos da sociedade que constantemente vem sendo vítimas destes delitos e em muitos dos casos, não sabem como agir, a quem recorrer, também tem por pretensão alcanças os acadêmicos de direitos, operadores de direito e pessoas das diversas áreas, despertando o interesse de todos a respeito desta forma criminal que muito se deve à modernização da sociedade e dos seus meios tecnológicos.

CAPÍTULO 1 - EVOLUÇÃO HISTÓRICA

1.1 Evolução Histórica da Informática

Mudanças na tipicidade e formas de praticar os crimes se enquadram de acordo com cada época e cultura vivida pela humanidade e para isso se faz importante lembrarmos um pouco da evolução tecnológica que vivemos nos últimos séculos.

Quando falamos de informática é necessário lembrar que os primeiros dispositivos criados tinham o objetivo de calcular, como por exemplo, o Ábaco[1]. Sua criação foi por volta do século VIII a.C . Na região da Mesopotâmia com o intuito de facilitar o trabalho do homem no processo de informações sendo o primeiro dispositivo manual de cálculo para o sistema decimal. O Ábaco até hoje é utilizado, não com a mesma necessidade que na época de sua criação, mas como demonstrativo, em escolas, para mostrar como esses instrumentos eram utilizados antes de haver toda a tecnologia atual, inclusive existem vídeos na internet explicando as funcionalidades do ábaco.

Mais de dois mil anos após, em 1642 foi criada pelo matemático Blaise Pascal, com apenas vinte anos de idade na época, a calculadora mecânica, conhecida como Pascalina[2], primeiro instrumento a fazer somas e subtrações**,** é a calculadora decimal conhecida com maior longevidade e sem dúvida tratava-se de um grande avanço se comparada com o ábaco. Porém, só em 1946 foi apresentado ao mundo o ENIAC (*Electronic Numerical Integrator and Computer*)[3], por uma equipe da Universidade de Pensilvânia coordenada por Herman Goldstine. É conhecido como o primeiro computador, era uma máquina que utilizava grande quantidade de recurso para fazer o que hoje em dia é feito por minúsculos microchips.

Os projetistas do ENIAC queriam usar o novo computador para ajudar a prever o tempo ou o mercado de ações, mas acabou auxiliando o principiante programa espacial americano a sair do chão[4].

---

[1] **Ábaco,** formado por fios paralelos e contas ou arruelas deslizantes, que de acordo com a sua posição, representa a quantidade a ser trabalhada, contém 2 conjuntos por fio, 5 contas no conjunto das unidades e 2 contas que representam 5 unidades.

[2] KLEINA, Nilton. **Colossus: herói da guerra e um dos primeiros computadores do mundo**. Tecmundo, 14 de junho de 2013. Disponível em:<http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 02/06/15.

[3]**MUSEU DO COMPUTADOR.** Universidade Estadual de Maringá. Disponível em: <http://www.din.uem.br/museu/hist_nomundo.htm>. Acesso em: 02/06/15.

[4] BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006. p. 273.

Finalmente, o ENIAC foi desligado pela última vez em 1955 sendo substituído pelo UNIVAC (*Universal Automatic Computer - Computador Automático Universal*). Bem menor do que o ENIAC, com as mesmas dimensões de uma geladeira doméstica, o UNIVAC era mais rápido e mais flexível do que o seu antecessor, sendo o primeiro a ser produzido em série, foi considerado o primeiro computador eletrônico, no entanto, é a imagem do enorme ENIAC que a população associa sempre como "primeiro" e pouco se ouviu falar no seu substituto. Mesmo sendo menor e, mas barato, o ENIVAC ainda era regalia de poucos por conta do seu preço, ficando restrito a laboratórios e universidades.

Sabe-se hoje que na mesma época da criação do ENIAC, na Inglaterra, Alan Turing[5] coordenava a construção de calculadores eletromecânicos semelhantes aos criados na América, destinados a decifrar as mensagens das Forças Armadas Alemãs. Sendo uma das figuras mais importantes da computação, Alan Turing focou sua pesquisa na descoberta de problemas formais e práticos que poderiam ser resolvidos através de computadores. Para aqueles que apresentavam solução, foi criada a famosa teoria da "Máquina de Turing", que, através de um número finito de operações, resolvia problemas computacionais de diversas ordens. A máquina de Turing foi colocada em prática através do computador *Colosssus*[6] em 1946.

Por sua vez, na Alemanha Konrad Zuse[7], sem grandes apoios oficiais, criava calculadores eletromecânicos para cálculo de armamento da Força Aérea Alemã. Sendo o primeiro a desenvolver uma máquina de cálculo de controle automático Zuse, depois de muitas tentativas, chegou à conclusão de que o calculador somente necessitaria de três unidades básicas, quais sejam: uma controladora, uma memória e um dispositivo de cálculo. Por motivo da pré-guerra ele teve que abandonar as suas pesquisas e alguns dos seus trabalhos foram destruídos juntamente com a sua casa em um bombardeio no ano de 1944. Com isso percebemos que em lugares diferentes, porém em épocas semelhantes, estavam sendo construídos equipamentos tecnológicos com objetivos parecidos. Esses são os precursores das máquinas que conhecemos hoje.

---

[5] FONSECA FILHO, Cléuzio. **História da Computação: O Caminho do Pensamento e da Tecnologia.** Porto Alegre : Edipucrs, 2007. p. 74.

[6] KLEINA, Nilton. **Colossus: Herói da Guerra e um dos Primeiros Computadores do Mundo**. Tecmundo, 14 de junho de 2013. Disponível em:<http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 02/06/15.

[7] FONSECA FILHO, Cléuzio. **História da Computação: O Caminho do Pensamento e da Tecnologia.** Porto Alegre : Edipucrs, 2007. p. 101.

Só então na década de 1970 surgiram os computadores pessoais[8], eles tiveram que se tornarem menores e mais baratos, passando a fazer todo tipo de serviços e não apenas de comunicação ou guerra. Apesar da nomenclatura de "computadores pessoas", as máquinas que a princípio era privilégio dos Americanos, continuavam sendo objeto de poucos, pois em alguns países, ainda hoje, é um artigo de luxo, então o que dirá na época do seu surgimento?

Segundo o Museu da História do Computador [9] (*Computer History Museum*), o primeiro "computador pessoal" foi o Kenbak-1, lançado em 1971. Tinha 256 *bytes* de memória e foi anunciado na revista *Scientific American* por US$ 888; todavia, não possuía CPU e era, como outros sistemas desta época, projetado para uso educativo (ou seja, demonstrar como um "computador de verdade" funcionava). Em 1975, surge o Altair 8800[10], um computador pessoal baseado na CPU Intel 8080. O Altair 8800 revolucionou tudo o que era conhecido como computador até aquela época. Com um tamanho que cabia facilmente em uma mesa e um formato retangular, também era muito mais rápido que os computadores anteriores. O projeto usava um processador 8080 da Intel, potencializando o seu desempenho, pois esse tipo de processador era moderno na época. A IBM (*International Business Machines)*, por sua vez, lançou em junho de 1979 o computador pessoal PC-XT, com capacidade de executar 750.000 funções por segundos, dezenove anos depois foi mostrado ao mundo o *Pentium III*, com uma capacidade ainda maior, pois este podia executar mais de 400 milhões de operações por segundos[11].

Mas foi com o jovem Bill Gatts, ao tempo aluno da universidade de Havard, e o revolucionário, Steve Jobs que o mundo abriu as portas para a cibernética. Com seus olhares inovadores foram os mais famosos personagens da historia da informática ao dar início a duas gigantes empresas, a Microsoft[12] e a Apple[13].

---

[8] MORIMOTO, Carlos E. **O Surgimento dos Computadores Pessoais**. Guia do hardware. 01 de janeiro de 2002. Disponível em: <http://www.hardware.com.br/livros/hardware-manual/surgimento-dos-computadores-pessoais.html>. Acesso em: 03/06/15.

[9] **COMPUTER HISTORY MUSEUM**. Disponível em:<http://www.computerhistory.org/revolution/personal-computers/17/297>.Acesso em: 03/06/15.

[10] FONSECA FILHO, Cléuzio. **História da Computação: O Caminho do Pensamento e da Tecnologia.** Porto Alegre: Edipucrs, 2007. p. 130.

[11] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** São Paulo: Saraiva. 2000.
Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 1. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

[12] **Microsoft Corporation** é uma empresa transnacional estadunidense com sede em Redmond, Washington, que desenvolve, fabrica, licencia, apoia e vende softwares de computador, produtos eletrônicos, computadores e serviços pessoais.

[13] **Apple Inc**. é uma empresa multinacional norte-americana que tem o objetivo de projetar e comercializar produtos eletrônicos de consumo, software de computador e computadores pessoais.

Bill Gatts ao perceber que as máquinas não tinham grande funcionalidade se não possuísse um sistema operacional, interessou-se pelo novo sistema e com isso tornou-se um grande percursor criando linguagens de programação. O sucesso do Altair fez com que o jovem programador quisesse trabalhar na máquina, criando a sua linguagem própria, a Altair Basic. Também inspirado por o Altair, Steve Jobs (fundador da Apple) sentiu que ainda faltava algo no projeto daquela máquina e apesar de suas funcionalidades, este computador não era fácil de ser utilizado por pessoas comuns, pois, para Steve, um computador deveria representar de maneira gráfica o seu funcionamento, ao contrário de luzes que acendiam e apagavam. Por isso, o Apple I[14], lançado em 1976, o mais parecido com a imagem de um computador que temos hoje, ele podia ser ligado diretamente a um aparelho de televisão, que exibia o que estava acontecendo no computador. Como o sucesso da máquina foi muito grande, em 1979 foi lançada o Apple II, que seguia a mesma ideia.

Seguindo na mesma linha, os computadores Lisa (1983) e Macintosh (1984)[15], foram os primeiros a usar o mouse e possuir a interface gráfica como nós conhecemos hoje em dia, com pastas, menus e área de trabalho, tornando-se um grande sucesso de vendas. Paralelamente à Apple, Bill Gates fundou a empresa Microsoft, que também desenvolvia computadores. No começo de sua existência, final dos anos 1970 e até meados dos anos 1980, Gates usou as ideias contidas nas outras máquinas para construir a suas próprias, como mostrado no entendimento de Briggs e Burke.

> Era óbvio, em 1984, quando havia somente menos de um milhão de máquinas em uso no mundo, muitas delas incompatíveis entre si e todas se tornando rapidamente obsoletas, que os programas eram a chave para aumentar o uso dos computadores, fossem eles pessoais ou de empresas, pequenos ou grandes. A Microsoft rapidamente se transformou no maior fornecedor do ramo, quando seu sistema operacional Windows foi distribuído para o mundo todo[16].

Utilizando processadores 8086 da Intel, o primeiro sistema operacional da Microsoft, o MS-DOS, estava muito aquém dos desenvolvidos por Steve Jobs, por esse motivo, Bill Gates acabou criando uma parceria com Jobs e, após algum tempo, copiou toda a tecnologia gráfica do Macintosh para o seu novo sistema operacional, o Windows. Desta forma, em meados de 1980, O Machintosh e o Windows se tornaram fortes concorrentes. Com a demissão de

---

[14] MORIMOTO, Carlos E. **O Apple 1: Guia do Hardware**. 04 de agosto de 2011. Disponível em < http://www.hardware.com.br/guias/historia-informatica/apple.html>. Acesso em: 04/06/15.
[15] MORIMOTO, Carlos E. **O Lisa e o Macintosh: Guia do hardware**. 10 de agosto de 2011. Disponível em <http://www.hardware.com.br/guias/historia-informatica/lisa-macintosh.html>. Acesso em: 04/06/15.
[16] BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006. p. 283.

Steve Jobs da Apple, a empresa acabou muito enfraquecida. Assim, a Microsoft passou a se tornando líder do mercado de computadores pessoais.

Do aparecimento do ENIAC até os aparelhos atuais passarem-se apenas 69 anos, quanto ao acesso muito mudou, pois antes eram prioridades das grandes empresas e hoje, com o avanço no mercado mundial de consumo, muitas pessoas têm possibilidade de possuir um aparelho eletrônico que permite ter acesso a informações e dados. Esses novos aparelhos diferem não só apenas no tamanho, mas também no valor, funcionalidade e acessibilidade dos usuários.

No Brasil a era da informática começou nos anos de 1950, em 1957, chegou ao Brasil o primeiro computador, um Univac-120, adquirido pelo Governo do Estado de São Paulo, era usado para calcular todo o consumo de água na capital. Nesta época se fazia necessário à importação de tecnologia de países como os Estados Unidos e Japão, tratava-se de máquinas enormes que eram utilizadas apenas nas grandes empresas, universidades e órgãos governamentais, por conta do seu preço elevado e tamanho, poucos setores tinham acesso a essas máquinas, apenas em 1959 é que foi comprado o primeiro computador por uma empresa privada brasileira. A empresa Anderson Clayton compra um Ramac 305 da IBM.

Não havia fabricantes nacionais até então, e só a partir do trabalho de algumas universidades: como a universidade de são Paulo (USP), a Católica do Rio de Janeiro e a Estadual de campina que foram criados projetos nesse setor, e no ano de em 1972 foi construído na USP o primeiro computador nacional, "o patinho feio", ainda nesse ano, buscando uma independência tecnologia, os militares e os meios científicos criaram a CAPRE (comissão de coordenação das atividades de processamento eletrônico).

A Universidade de São Paulo (USP) e a Pontifícia Universidade Católica (PUC) do Rio de Janeiro, no ano de 1974 receberam incentivos da Marinha de Guerra para a criação do projeto G-10, tratava-se de um projeto voltado para a criação de equipamentos de eletrônica de bordo e neste mesmo ano foi que surgiu a primeira empresa brasileira de fabricação de computadores, a COBRA (Computadores Brasileiros S.A). Tratava-se de uma empresa estatal que tinha como objetivo transformar o G-10 em um produto de consumo nacional. O COBRA 530, lançado no início da década de 1980, foi o primeiro computador totalmente projetado, desenvolvido e industrializado no Brasil.

Cinco anos depois da elaboração pela PUC e USP do projeto G10, foi criada pelo governo uma política de reserva de mercado para a fabricação de aparelhos de informática, a SEI (Secretária Especial de Informática) com o objetivo de desenvolver uma indústria local e

obter tecnologia de ponta, substituindo assim à antiga CAPRE. Com a criação da Lei n° 7232, em 1984, oficializou-se a reserva para alguns seguimentos do mercado, inclusive softwares. Através destes incentivos governamentais a indústria de informática nacional chegou a atingir taxas de crescimento de 30% ao ano em meados de 1980, com isso em 1986 o Brasil alcançou a 6° posição no mercado mundial de informática e de 5° maior fabricante.

Nos anos de 1990 ocorreram modificações na política nacional de informática, a (PNI), visando o engajamento nas políticas econômicas liberais e dando mais abertura ao mercado exterior, pois o Brasil vinha sofrendo sanções comerciais em virtude da falta de abertura do mercado nacional para a concorrência estrangeira, também estavam ocorrendo reclamações de diversos setores comercias a respeito do atraso tecnológico brasileiro e dos altos preços provocados pela reserva de mercado[17].

Atualmente a informática no Brasil já alcançou o seu lugar no mercado, não só com as empresas criadoras dos hardwares e softwares, mas também no mercado de consumidores e usuários que hoje é um dos maiores do mundo. Segundo dados da Associação Brasileira das Empresas de Software[18] (*ABES software*), a Indústria Brasileira de Tecnologia da Informação está posicionada em 8º lugar no ranking mundial.

Todo esse aumento e modernização da tecnologia têm influenciado diretamente na forma como os crimes são praticados, pois esses utensílios modernos têm erroneamente servido como ferramentas para a prática de delitos, muitos destes, antes cometidos com o auxilio de armas, hoje são feitos através ou auxiliados por aparelhos tecnológicos que não têm como função principal a prática de nenhum crime, mas que, da mesma forma como no tempo em que surgiram os primeiros computadores e tiveram a sua função substituída para fins de auxiliar nas guerras, agora vemos que essas máquinas estão tendo a sua função principal desviada novamente, e atualmente com a finalidade criminosa.

Porém para que haja a proliferação dos crimes cibernéticos se fez necessário um fator primordial, a internet. Foi com o advento desta que as máquinas aumentaram a possibilidade de transportar informações e ocultar a figura do autor de um crime, facilitando assim a prática desses delitos. Sendo assim, para melhor entendermos como esses delitos são possíveis precisamos analisar o fenômeno da internet.

---

[17]**MUSEU DO COMPUTADOR** Universidade Estadual de Maringá. Disponível em: < http://www.din.uem.br/museu/hist_nobrasil.htm>. Acesso em: 02/06/15.

[18] **MERCADO BRASILEIRO DE SOFTWARE: PANORAMA E TENDÊNCIAS**. 1. ed. São Paulo: ABES - Associação Brasileira das Empresas de Software, 2015. Disponível em: < http://central.abessoftware.com.br/Content/UploadedFiles/Arquivos/Dados%202011/ABES-Publicacao-Mercado-2015-digital.pdf> acesso em: 02/06/15.

1.2 Evolução Histórica da Internet

No final de Outubro de 1957 ocorreu um evento que iria mudar o mundo. A União Soviética lançou com sucesso o primeiro satélite na órbita da Terra. Chamado "Sputnik 1", ele chocou o planeta, especialmente os Estados Unidos, que tinha seu próprio programa de lançamento de satélites, mas ainda não o havia lançado. Mas o que isso tem haver com internet? Tem haver que este evento levou diretamente à criação da ARPA (Agência de Projetos de Pesquisa Avançada) do Departamento de Defesa dos Estados Unidos, devido a uma reconhecida necessidade de uma organização que possa pesquisar e desenvolver tecnologia avançada. Talvez o seu mais famoso projeto (certamente o mais amplamente utilizado) foi à criação da Internet.

A internet trata-se de um sistema global de redes de computadores, que através dele é possível a comunicação e transferência de arquivos entre as máquinas ligadas a ela, possibilitando uma troca de informações, de maneira rápida, em rede[19]. Surgiu na década de 1960 com a criação da ARPANET (*Advanced Research Projects Agency Network*)[20], Foi a primeira rede de computadores desenvolvida pela agência americana ARPA em Setembro de 1969, o plano para esta rede de computadores foi apresentado em Outubro de 1967, e em Dezembro de 1969 a primeira rede de quatro computadores estava pronta e funcionando.

O grande problema em criar uma rede era como conectar redes físicas separadas sem que as ligações aumentem os recursos de rede para links constantes. A técnica que solucionou este problema é conhecida como troca de pacotes e envolve requisições de dados sendo divididos em pequenos pedaços "pacotes"[21], que podem ser processados rapidamente sem bloquear a comunicação de outras partes, este princípio ainda é usado para o funcionamento da Internet hoje.

Como citada anteriormente, a formação da ARPA se deu no ano de 1958 pelo departamento de defesa dos Estados Unidos tendo como objetivo alcançar superioridade tecnológica militar em relação à União Soviética na marca do lançamento do primeiro Sputnik, sendo totalmente financiada pelo governo Norte-Americano, durante o período que ficou conhecido como Guerra Fria. Temendo um ataque por parte dos seus opositores, os americanos tinham

---

[19] CORRÊA, Gustavo Testa**. Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 8. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

[20] BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006. p. 301.

[21] Ibidem. p. 301.

como objetivo desenvolver uma rede de comunicação que não os deixasse vulneráveis, caso houvesse algum ataque soviético ao Pentágono. Usando um *Backbone* (redes conectoras), que passavam por baixo da terra, a ARPANet ligava os militares e os investigadores sem ter um centro definido ou mesmo uma rota única para as informações.

No início da década de 1970, universidades e outras instituições que faziam trabalhos relacionados com a defesa, tiveram permissão para se conectarem à ARPANet, era uma rede limitada, utilizada entre os alunos de universidades e institutos de pesquisa, sendo que poucos anos depois já havia dois mil usuários, e em meados de 1975 existiam aproximadamente 100 sites. A visão dos usuários era que a internet oferecia acesso livre, pois qualquer computador podia ser ligado a ela de qualquer lugar e a mesma sobreviveria à retirada ou destruição de algum computador da sua rede.

Na época as mensagens de E-mail era a base das comunicações e tratavam de todo os tipos de assunto e não apenas dos relacionados à defesa e segurança, nesse mesmo período o sinal @ (arroba) foi introduzido nos endereços com o simples objetivo de separar o nome dos usuários dos endereços dos E-mails, também surgiram às abreviações "*com*" para comercial e "*mil*" para militar se estabelecendo em 1986[22].

O primeiro provedor de internet pago foi o COMPUSERVE, que começou a operar em 1979 para um "clube privado" de pessoas, tendo em seguida como concorrente a AMERICAN ON-LINE, um provedor ligado a grupos alemães e franceses, e por fim surgiu um terceiro concorrente, o PRODIGY. Em 1993, os três rivais tinham um conjunto de assinantes que haviam duplicado em dois anos, até os 3,5 milhões[23].

Mas foi Berners-Lee, eleito pela revista TIME como sendo o "único pai da *Web*" que em 1989 criou o World Wide Web (www)[24], ou seja, teia mundial, com a intenção de preservar a internet sem proprietários, aberta e livre; o oposto dos empreendedores norte-americanos que visavam lucro. Juntamente com o desenvolvimento dos navegadores, ela é considerada a principal responsável por a popularização da internet, proporcionando aos usuários a utilização de imagens, movimentos e sons[25].

A *Web* (do inglês "teia") trata-se de um sistema hipertextual que opera através da internet, é um meio de comunicação global no qual usuários podem ler e escrever através

[22] BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006. p. 301.
[23] Ibid. p. 301.
[24] Ibidem, p. 302.
[25] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 10. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

de computadores conectados à Internet. O termo Web é usado erroneamente como sinónimo da própria Internet, sendo a Web apenas um serviço que utiliza a Internet, assim como as mensagens de e-mail.

Já naquela época, tornou-se notório que Berners-Lee popularizou um instrumento de comunicação poderoso, que antes era privilégio apenas da elite, deixando muitos insatisfeitos com essa popularização, ou seja, nem todos estavam entusiasmados com essa massificação da internet, pois temiam que, com o aumento e popularização dos usuários, acarretaria na desqualificação das informações e na forma como eles as utilizavam, pois para os usuários pioneiros da Arpanet, que eram a minoria, quanto mais usuários da internet houvesse, mais terreno inútil existiria, ou seja, já naquela época notava-se que a proliferação da internet poderia acarretar um mau uso por parte dos usuários[26]. Era previsto que a internet liberava e dava poderes aos indivíduos, mas talvez naquela época o que não imaginariam era quão grande o poder que ela traria como bem comparou Briggs e Burke.

> Havia abordagens muito contrastantes sobre o futuro da Internet. Assim como nas ferrovias, ela reuniria estranhos: você nunca sabia quem iria encontrar. Semelhante à mídia — e pela mídia —, ela oferecia informação, entretenimento e educação. Ao contrário de tudo isso, porém, cresceria a partir de baixo, sem direcionamento por parte do governo. Isso era um atrativo, mesmo para os críticos. Mas poderia a Internet continuar assim[27]?

A internet no Brasil se desenvolveu em meados de 1990 no meio acadêmico e científico. No seu início, o acesso era restrito a professores e funcionários de universidades e instituições de pesquisa. Somente no ano de 1995 a internet deixou de ser privilégio das universidades e da iniciativa privada para se tornar de acesso público.

Desde então o número de provedores que oferecem o serviço e número de usuários que utilizam este recurso aumentam a cada ano e passou a ser utilizada em quase todas as atividades da vida cotidiana, sendo um dos meios de comunicação mais utilizados, esse crescimento de usuários tem como escopo principal a mudança de conteúdo que, com o passar do tempo, ocorreu na rede, ou seja, passou-se de simples arquivos de textos a uma forma de comunicação com vídeos sendo enviados em momento real, com grande qualidade de conexão[28].

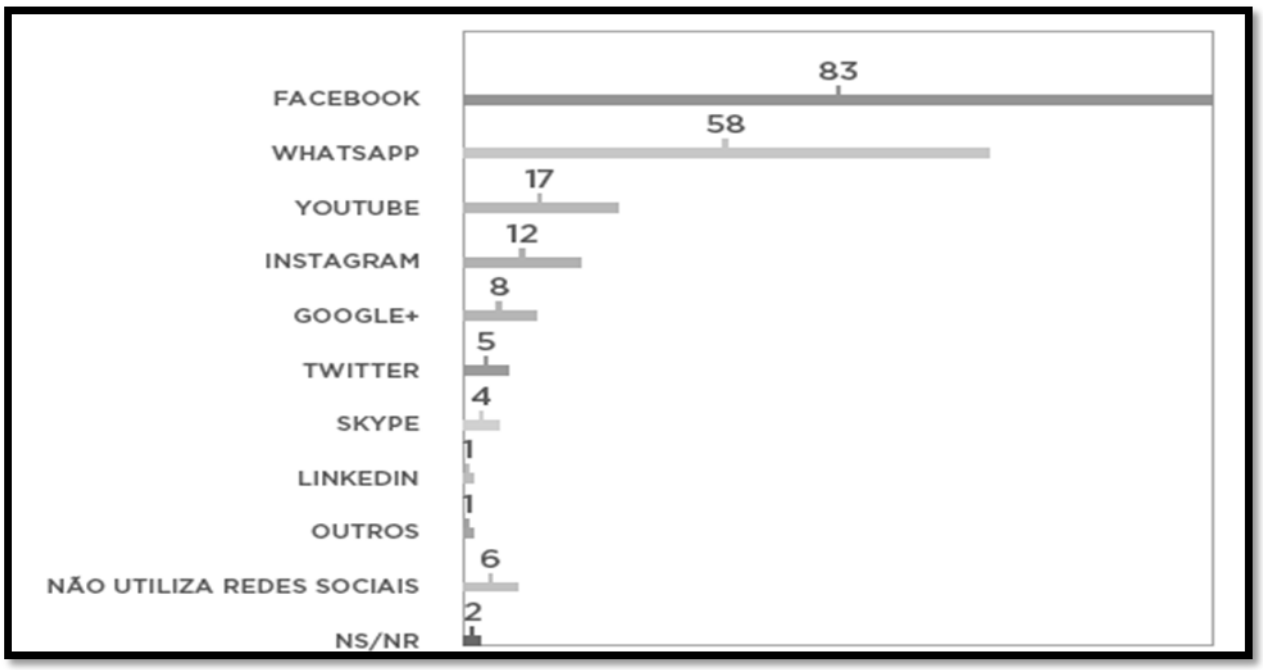
---

[26] BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006. p. 302.
[27] Ibidem, p. 303.
[28] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 9. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

O uso das redes, atualmente, é objeto de interesse de pessoas de todas as idades e graus de escolaridade, pois, com bem sabemos, no século XXI foram disseminados os chamados sites de redes sociais, onde qualquer pessoa pode criar um perfil e ficar em contato com outros internautas, podendo promover desde conversas banais a revoluções, a privacidade se tornou um artigo de luxo, já que qualquer usuário pode acessar a rede e ver informações diversas.

Entre os entrevistados pela Pesquisa Brasileira de Mídia 2015, realizada pela Secretaria de Comunicação Social da Presidência da República, que usam a internet, afirmaram que as redes sociais e os programas de trocas de mensagens instantâneas mais usadas estão o Facebook com 83%, em seguida vem o Whatsapp com 58%, o Youtube com 17%, o Instagram com 12% e o Google com (8%). O Twitter, popular entre as elites políticas e formadores de opinião, foi mencionado apenas por 5% dos entrevistados como bem mostra o gráfico a seguir[29].

GRÁFICO 1 - Redes Sociais mais utilizadas.



O gráfico acima aponta um demonstrativo das preferências atuais dos internautas em geral, não selecionando aqui por faixa etária, região ou nível de escolaridade, por exemplo.

Esse gráfico mostra bem o perfil do usuário de internet no Brasil, sua grande maioria tem por objetivo relações social, e muitas das vezes confiam cegamente em desconhecidos, o

[29]**LISTA DE PESQUISAS QUANTITATIVAS DE CONTRATOS ATUAIS**. Disponível em: <http://www.secom.gov.br/atuacao/pesquisa/lista-de-pesquisas-quantitativas-e-qualitativas-de-contratos-atuais/pesquisa-brasileira-de-midia-pbm-2015.pdf/view>. Acesso em: 01/06/15.

que faz das redes sociais uma porta de entrada para a prática de crimes, sendo assim, a Internet, que é um ambiente social, pode tornar uma pessoa popular bem como, denegrir sua reputação. Mas ela não se limitou a redes sociais e site de compras, pois bem sabemos que a mesma desempenha um papel fundamental na educação, com o advento de sites educativos, cursos a distancia e também nas indústrias realiza um papel fundamental, pois boa parte dos equipamentos tecnológicos tem sua operação e funcionamento interligados à rede.

A chegada da internet ao Brasil[30] se deu nos anos de 1980, em 1987, realizou-se uma reunião na Universidade de São Paulo, na qual estavam presentes representantes do governo e da Embratel, com o objetivo de criar redes interligando a comunidade acadêmica e científica brasileira com outros países tendo a intenção de trocar informações.

O Laboratório Nacional de Computação Científica (LNCC) conseguiu se conectar à Universidade de Maryland, nos Estados Unidos, em 1988 acessando a Bitnet (*Because It's Time Network*), uma rede que permitia a troca de mensagens. No mesmo ano, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) se conectou, também por meio da Bitnet, da cidade de São Paulo, ao Fermilab (*Fermi National Accelerator Laboratory*), um laboratório especializado em física de partículas de energia em Chicago nos Estados Unidos.

A Universidade Federal do Rio de Janeiro também se conectou à Bitnet, em 1989, através de uma universidade americana, tornando-se a terceira instituição a ter acesso a essa tecnologia. Nesse ano, foi criada, com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), a Rede Nacional de Pesquisa (RNP), que durante a década de 1990 foi a responsável por fornecer acesso à internet a aproximadamente 19600 instituições, com cerca de 65 mil usuários.

No ano de 1991, o acesso à rede de informações, já era utilizada também por órgãos do governo e instituições educacionais de pesquisa. Nessa época a internet era utilizada para transferências de arquivos, debates e acesso a base de dados nacionais e internacionais. Em 1992, ocorreu a implantação de uma rede que cobria grande parte do país. Inicialmente interligava onze estados, uma rede de equipamentos e linhas de comunicação que compunham o que se pode chamar de central da RNP.

Nos anos seguintes seguiu o processo de divulgação dos benefícios da internet entre os estudantes e empresas privadas. Em 1994, alunos da USP criaram inúmeras páginas na Web, estima-se que mais da metade existentes no país haviam sido elaborados pelos mesmos. Somente em 1995, foi realizada a primeira transmissão à longa distância entre os estados, reali-

[30]**MUSEU DO COMPUTADOR**. Universidade Estadual de Maringá. Disponível em: < http://www.din.uem.br/museu/hist_nobrasil.htm>. Acesso em: 02/06/15.

zada por São Paulo e Rio Grande do Sul, e finalmente neste mesmo ano foi liberada a operação comercial no Brasil, mas ainda assim sem alcançar grande desenvolvimento.

No mesmo ano, foi criado o Comitê Gestor da Internet no Brasil, com a atribuição de coordenar e integrar todas as iniciativas de serviços relacionados à Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados[31], além de estabelecer os padrões pelo qual o endereço eletrônico ou nome são apresentados na internet, padrões estes estabelecidos pelo protocolo DNS (*domain name system*), conhecido também por domínio. Tais requisitos são regulamentados no país pelo Comitê Gestor de Internet do Brasil, através da resolução nº 1, de 15 de abril de 1998[32].

Atualmente a internet é utilizada em quase tudo que fazemos, estamos tão familiarizados, que isso passou a ser algo inerente à vida cotidiana, sendo quase impossível praticar muitas das atividades diárias sem ela. Não resta dúvida que foi o grande invento do século XX, porém isso que nos trouxe tantos benefícios e comodidades inseriu nossa sociedade em um novo senário criminal que seria inimaginável há décadas atrás, pois falar em crime nos faz remontar a figura do criminoso, mas quem seria esse criminoso que com o advento da internet não vemos o "seu rosto"?

De acordo com a Pesquisa Brasileira de Mídia, realizada pela Secretária de Comunicação Social da Presidência da República em 2015, quando se analisam os dados da pergunta sobre qual meio de comunicação o entrevistado utiliza mais. A internet foi apontada por 42% dos brasileiros[33]. Entre os usuários, a exposição é intensa e com um padrão semelhante, onde a grandes maiorias acessam a internet todos os dias, com uma exposição média diária de 4h59 de 2ª a 6ª-feira e de 4h24 nos finais de semana. O pico de uso da internet ocorre à noite, por volta das 20 horas[34].

No Brasil, as características sociodemográficas da população têm um grande impacto no uso da internet, principalmente se comparada aos outros meios de comunicação. Renda e escolaridade criam um hiato digital entre quem é um cidadão conectado e quem não é. Já os elementos geracionais ou etários mostram que os jovens são usuários mais intensos das novas

---

[31] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 17. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

[32] Ibidem, p. 18.

[33] **LISTA DE PESQUISAS QUANTITATIVAS DE CONTRATOS ATUAIS.** Disponível em: <http://www.secom.gov.br/atuacao/pesquisa/lista-de-pesquisas-quantitativas-e-qualitativas-de-contratos-atuais/pesquisa-brasileira-de-midia-pbm-2015>. Acesso em: 01/06/15.

[34] Ibid.

mídias, pois 65% dos usuários são jovens com até 25 anos e acessam internet todos os dias. Entre os que têm acima de 65 anos, esse percentual cai para 4%.

Por sua vez, a análise por escolaridade mostra que 87% dos entrevistados com ensino superior acessam a internet pelo menos uma vez por semana, enquanto apenas 8% dos entrevistados que estudaram até 5ª ano do Ensino Fundamental o fazem com igual frequência[35], quanto ao objetivo, o entretenimento ainda continua sendo o maior motivo para o uso, como mostrado no gráfico da Pesquisa Brasileira de Mídia realizada em 2015[36].

GRÁFICO 2 - Motivos do uso da Internet.

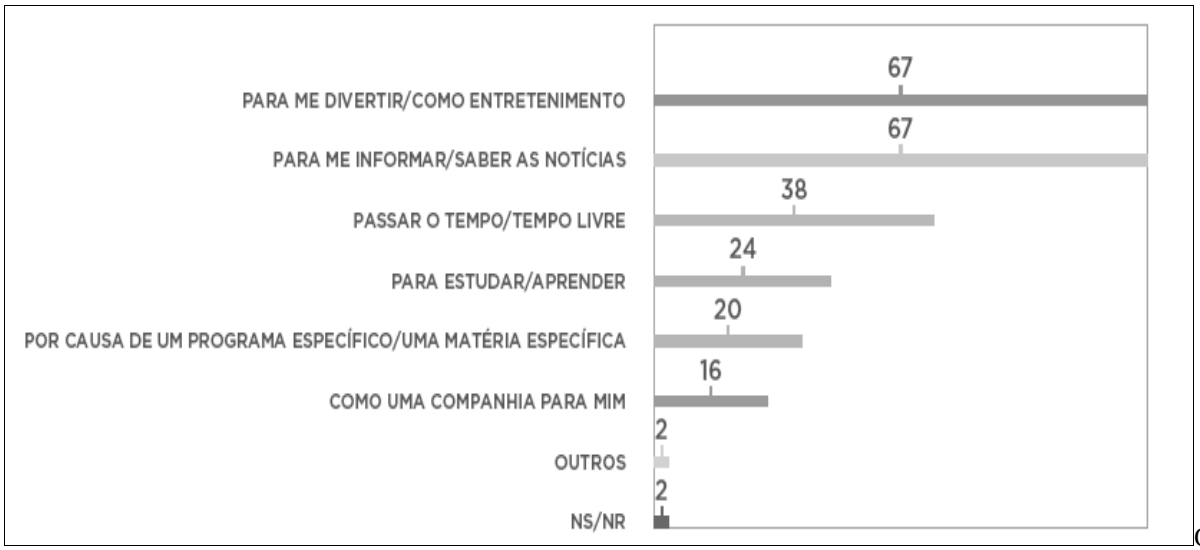


Gráfico que retrata os motivos pelos quais os entrevistados fazem preferência ao uso da internet em relação a outras formas de entretenimento.

O perigo de se usar tanto a internet como divertimento gira em torno da perda de noção que muitas vezes o usuário acaba tendo em relação aos perigos, se deixando levar por propagandas enganosas, sites maliciosos, anúncios falsos ou pessoas mal intencionadas, acabam criando uma espécie de falsa proteção por força do hábito, do costume de sempre está ali, no conforto de sua casa por traz da tela de um aparelho achando que nada de errado vai acontecer, confunde a segurança do espaço físico com a do espaço virtual, e neste nem sempre estamos seguros.

Na internet pode-se também haver inúmeras informações totalmente desnecessárias. É possível publicar comentários sobre uma determinada pessoa, denegrir sua imagem, como também há roubo de identidade, calúnia, enfim, tantas outras coisas. O que não se pode es-

[35] **LISTA DE PESQUISAS QUANTITATIVAS DE CONTRATOS ATUAIS.** Disponível em: <http://www.secom.gov.br/atuacao/pesquisa/lista-de-pesquisas-quantitativas-e-qualitativas-de-contratos-atuais/pesquisa-brasileira-de-midia-pbm-2015>. Acesso em: 01/06/15.
[36] Idem.

quecer é que os crimes virtuais ainda são poucos solucionados, então, o melhor mesmo é a precaução.

1.3 Evolução Histórica do Crime Cibernético

A literatura científica internacional demonstra que o universo dos crimes informáticos teve seu início no século XX mais precisamente em 1960 onde se deu as primeiras referências sobre essa modalidade de crimes nas mais diversas denominações, com maiores incidências em casos de manipulação e sabotagem de sistemas de computadores. A primeira notícia de crime cibernético se deu no ano de 1964, no MIT (*Massachusets Institute of Technology*), o crime foi praticado por um aluno de 18 anos, tendo o mesmo recebido apenas uma advertência pelo ato cometido[37]. Em 1969, Aaron M. Kohn intitulou de "Crime de computador" seu editorial publicado no *The Journal of Criminal Law, Ciminology and Policy Science*, utilizando-se da expressão, crimes de computados, para designar os seus praticantes[38]. Já Jean Pradel e Cristian Feuillard denominaram os mesmo atos de "infrações cometida por meio do computador". "Criminalidade informática, foi o termo utilizado por Klaus Tiedermann ao designar as formas de comportamento ilegal que se possa ser realizado por intermédio da tecnologia". Segundo Ferreira, ao explicar o assunto, traz-nos a concepção de Ulrich Sieber de que:

> [...] O surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos, constituídos sobre tudo por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados, sobretudo em matérias jornalísticas. Somente na década seguinte é que iriam iniciar-se os estudos sistemáticos e científicos sobre essas matérias, com o emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial, sabendo-se, porém da existência de uma grande cifra negra não considerada nas estatísticas[39].

Uma década depois, precisamente em 1970, a figura do Hacker já era citada com o advento de crimes como, invasão de sistema e furto de software, mas foi em 1980 que houve maior propagação dos diferentes tipos de crimes como a pirataria, pedofilia, invasão de sistemas, propagação de vírus, revelando uma vulnerabilidade antes não prevista pelos criadores destas tecnologias. Surge então, à necessidade de se despender maiores preocupações com a

---

[37] FERREIRA, Érica Lourenço de Lima. **Internet: Macrocriminalidade e Jurisdição Internacional.** Curitiba: Juruá, 2007. p. 100.
[38] FERREIRA Ivette Senise. **Direito e Internet: Aspectos Jurídicos Relevantes**. 2. ed. Coord. Newton de Lucca; Adalberto Simão Filho e outros. São Paulo: Quartier Latin,2005. p. 238.
[39] Ibidem. p.239.

segurança virtual, exigindo-se uma atenção especial para identificação e punição dos responsáveis, que a essa altura estão em todos os lugares do mundo, como foi o caso da caça desesperada do governo americano atrás de Kevin Mitnick, um dos hackers mais famosos do planeta e que posteriormente passou a trabalhar para o governo na área da segurança da informação.

O conceito inicialmente atribuído ao delito de computador precisou ser ampliado para abranger condutas que anteriormente não eram consideradas como crimes informáticos, mas sim como crimes econômicos, patrimoniais ou contra a intimidade das pessoas, chegando-se só então, na década de 1990, a uma definição que entendeu o crime cibernético como sendo "qualquer comportamento ilegal, aético ou não autorizado, que envolva processamento automático de dados e/ou transmissão de dados"[40].

Com o passar dos anos e a popularização da tecnologia, novas condutas lesivas surgiram, aumentando com isso o campo da criminalidade informática, assim, ultrapassando as fronteiras nacionais dificultando a sua apuração e provocando maiores prejuízos às vitimas. No Brasil, a preocupação com esse assunto começou especialmente a partir das últimas décadas, com o aumento da popularização dessa inovação tecnológica, com isso manifestou-se a promulgação de algumas leis relativas à informática. A Constituição Federal de 1988, no seu art. 22, IV, fez menção à competência privativa da União para legislar sobre tal matéria. No entanto, continuou existindo lacunas na legislação existente, exigindo-se uma solução mais condizente com a gravidade da situação. Pensado nisso, foi instituído em 1984 pela Lei nº 7232, um Plano Nacional de Informática e também criado o Conselho Nacional de Informática e Automação com o objetivo de estabelecer princípios e diretrizes para uma Política Nacional de Informática. Com objetivo de proteger a propriedade intelectual sobre os programas de computador e sua comercialização no país, surgiu em 1987 a Lei nº 7646, disposições que foram depois revogadas pela Lei nº 9.609/98 que a substituiu.

Atualmente, de acordo com a Moderna Doutrina Penal, constitui crime de informática toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, caracterizando os elementos necessários para a criminalização das condutas puníveis, conceito este que pouco difere do atribuído na década de 1990. No entanto, respeitando o princípio da legalidade, o conceito de crime estará completo se a conduta do agente for ilícita e a responsabilidade penal puder ser atribuída pelas caracte-

[40] FERREIRA Ivette Senise. **Direito e Internet: Aspectos Jurídicos Relevantes**. 2. ed. Coord. Newton de Lucca; Adalberto Simão Filho e outros. São Paulo: Quartier Latin,2005. p 39.

rísticas que compõem a culpabilidade através de seus elementos essenciais[41], fatores estes que serão melhores analisados no capítulo seguinte.

[41] FERREIRA Ivette Senise. **Direito e Internet: Aspectos Jurídicos Relevantes**. 2. ed. Coord. Newton de Lucca; Adalberto Simão Filho e outros. São Paulo: Quartier Latin,2005. p. 240.

CAPÍTULO 2 - CONSIDERAÇÕES ACERCA DOS CRIMES CIBERNÉTICOS

A expressão crimes cibernéticos não é adotada de maneira uniforme pela doutrina, pois o mesmo delito, por muitas vezes, é denominado de formas diferentes, porém com um mesmo significado, tais como, "cibercrimes", "crimes virtuais", "crimes digitais", "crimes tecnológicos" e até mesmo "e-crimes", entre outros[42]. O crime cibernético possui características próprias, não se aplicando as mesmas dos crimes comuns, como por exemplo, a dispensa do contato físico entre o ofensor e a vítima, na maioria das vezes não exigindo grandes preparos, ocorrem em um ambiente sem povo, sem governo ou território, não gera sensação de violência e não há padrões para o seu acontecimento[43]. Trata-se de crimes cometidos através de equipamentos eletrônicos, contra os mesmos, ou através dele, sendo na sua grande maioria praticados com o auxílio da internet, utilizando-se de computadores e aparelhos tecnológicos, que possam ajudar na execução do delito, esses crimes também podem ocorrer no mundo real, porém no ambiente virtual adquirem peculiaridades, sendo assim, torna-se necessário uma adequação quanto ao seu tipo penal.

Algumas condutas utilizam os computadores como meio para o cometimento dos delitos, e há casos em que sem o uso do sistema informático seria impossível a sua consumação, sendo este uma ferramenta imprescindível, como por exemplo, a interceptação de e-mail que precisa de um ambiente informatizado para acontecer. Sendo assim, os crimes cibernéticos podem ser classificados em crimes cibernéticos próprios, onde o processamento eletrônico, o computador ou o sistema de informação é o alvo do delito; somente podem ser cometidos em meio eletrônico, como o acesso não autorizado a sistema de computadores e a disseminação de código malicioso e crimes cibernéticos impróprios, onde o sistema de computadores ou a internet é usado somente como mais um meio de execução do delito[44]. Neste capítulo falaremos sobre as fragilidades no meio informático, que com o auxílio destes torna-se possível a execução dos delitos informáticos, em seguida serão explanado alguns tipos de crimes cibernéticos, lembrando-se que só serão falados alguns, pois essa forma delitiva abrange diversos crimes, sendo assim, não seria conveniente tentar falar de todas. Finalizamos este capítulo

[42] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas.** 2. ed. São Paulo: Saraiva, 2015. p. 55.
[43] Ibidem. p. 59.
[44] Ibidem. p. 55.

com a análise do perfil da vítima e do autor do delito informático, sabendo que são partes fundamentais na existência destes.

2.1 Fragilidades do Mundo Cibernético

Para auxiliar a sociedade no seu desenvolvimento foi criado o computador e milhares de outros eletrônicos semelhantes, e nestes inventos foi inserida uma personalidade funcional, que são os softwares[45], com a chegada da internet e de lugares que não mais dependem do espaço físico das máquinas, como é o caso das nuvens de armazenamento[46], por exemplo; as formas que antes eram utilizadas no desenvolver as tarefas do dia a dia estão sendo substituídas em algum momento por tecnologias, mas como tudo isso, poderia sobreviver à modernidade sem romper em algum momento com a "perfeição"? Pois esse rompimento ocorre no instante em que o virtual é utilizado para a prática de atitudes ilícitas, que muitas vezes só é possível sua ocorrência por existir falhas técnicas e/ou humanas, que deixam espaços no sistema propiciando a invasão de pessoas mal intencionadas e à realização do delito.

Desde simples computadores pessoais até empresas de diversos portes precisam e armazenam dados, estas informações registradas em sistemas ou máquinas, circulando nas redes ou guardadas em espaços cibernéticos têm seu grau de importância, visto que o valor de determinado dado não se dá unicamente por estimativa econômica, mas também pessoais e afetivas, gerando com isso várias formas de se atribuir valores às informações.

Esses documentos podem ser acidentalmente prejudicados, por exemplo, quando acometidos por um problema técnico no sistema resultando no desaparecimento de registros pessoais, culminando em um prejuízo; como também podem ser alvo de ataques premeditados, por vírus[47] e/ou cracker[48] que desejam utilizar ou inutilizar aqueles dados, podendo ocorrer das mais diversas formas como, por exemplo, quando trazidos para o ambiente interno por intermédio de pen-drives ou CDS, ocasionando infecções no sistema operacional e nos programas, ou ainda, quando a ameaça vem do ambiente externo, invadindo o sistema ao simples clicar do mouse, ao tentar abrir uma mensagem de e-mail ou uma propaganda que contenha um link para a entrada de um vírus. Esses ataques têm diversas finalidades, como: roubo de

[45] **Software** é a parte lógica do computador.
[46] AMOROSO, Danilo. **O Que é Computação em Nuvem**. Tecmundo. 13 de junho de 2012. Disponível em:< http://www.tecmundo.com.br/computacao-em-nuvem/738-o-que-e-computacao-em-nuvens-.htm>. Acesso em: 01/10/15.
[47] **Vírus** é um software nocivo ao computador.
[48] Termo em inglês utilizado para denominar pessoa que tenha a intenção de prejudicar o sistema informático.

senhas, manipulação de imagens, acesso a informações em geral. Porém, a motivação que tem prevalecido ultimamente, é a finalidade financeira, diferente do que ocorria anteriormente onde o que objetivava os ataques dos hackers, era a manipulação e domínio dos sistemas visando à demonstração da sua superioridade quanto ao conhecimento tecnológico[49].

Crackers e Hackers são termos utilizados nos anos de 1990 para denominar pessoas aficionadas em informática, que dominavam as linguagens de programação e quase sempre se tratava de jovens criadores dos seus próprios vírus, tinha isso como um objetivo, ou seja, queriam saber o quanto era potente as suas invenções e para isso lançavam ataques a máquinas alheias, porém não era o seu objetivo principal causar prejuízo[50], no entanto é necessário distinguir esses dois personagens, pois há quem diga que cracker e hacker são as mesmas coisas, mas tecnicamente há diferenças: Os Hackers são pessoas que quebram senhas, códigos e sistemas de segurança por puro prazer em achar tais falhas. Preocupam-se em conhecer o funcionamento mais íntimo de um sistema computacional, ou seja, sem intenção de prejudicar ou invadir sistemas operacionais ou banco de dados, já o Cracker é o criminoso virtual que extorque pessoas usando seus conhecimentos, e as mais variadas estratégias, tendo como interesse basicamente o vandalismo[51]. De acordo com Kevin D. Mitnick.

> Alguns hackers destroem os arquivos ou unidades de disco inteiras das pessoas. Eles são chamados de *Crackers* ou *vândalos.* Alguns hackers novatos não se preocupam em aprender a tecnologia; eles apenas querem baixar as ferramentas dos hackers para entrar nos sistemas de computadores. Esses são chamados de *script kiddies.* Os hackers mais experientes, com habilidades em programação, desenvolvem programas para hackers e os postam na Web e nos sistemas de bulletin board. Em seguida, temos os indivíduos que não têm nenhum interesse em tecnologia, mas que usam o computador apenas como uma ferramenta que os ajuda a roubar dinheiro, bens ou serviço[52].

Em regra os indivíduos não sabem fazer a distinção entre um Crackers e um Hackers e os veículos de comunicação, ao divulgar ataques interpostos por estes, acabam por generalizar e refere-se a todos os ataques como sendo cometidos por hackers, e também no que se refere aos objetivos, o que parece ser uma unanimidade, é a motivação financeira, pois na maioria das vezes os ataques têm a pretensão de auferir lucro.

Importante destacar que, a ação de um indivíduo mal intencionado seria ineficaz caso não pudesse contar com um elemento crucial, por assim dizer, algo fundamental pra que haja

---

[49] Termo utilizado para referir-se às pessoas que se dedicavam ao conhecimento do sistema operacional, porém, atualmente passou-se, popularmente, a referir-se ao criminoso cibernético.
[50] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p.2.
[51] FERREIRA, Érica Lourenço de Lima. **Internet: Macrocriminalidade e Jurisdição Internacional.** Curitiba: Juruá, 2007. p.105.
[52] MITNICK, Kevin. D.; SIMON, Willian. L. **A Arte de Enganar - Ataques de hackers: controlando o fator humano na segurança da informação.** São Paulo: Person Education do Brasil Ltda, 2003. p. 01

o delito, estamos falando dos fatores técnicos e humanos, que por intermédio destes, o delito pode vir a se consumar.

2.1.1 Falhas Técnicas

A segurança no espaço cibernético tem como principal objetivo proteger as informações de quem se utiliza desse sistema, no entanto, por intermédio de falhas técnicas, essa segurança pode ser comprometida, e a se ver invadida, é que surge a consciência de que nunca se está completamente seguro em um ambiente virtual. A falsa sensação de segurança que o hábito de usar esses ambientes acaba proporcionando, muitas vezes leva a acomodação quanto aos cuidados técnicos que devem ser tomados em relação ao sistema e a mecanismos de segurança. Outro problema que acomete a proteção técnica do ambiente virtual, diz respeito ao constante surgimento de novas formas de ataques, fazendo com que o sistema de defesa se torne constantemente obsoleto, ou seja, para cada forma de proteção que é desenvolvida surge um novo tipo de ataque, existindo assim uma batalha constante.

Podemos dizer que o ambiente virtual está vulnerável quando este apresenta deficiências de segurança, tais como antivírus desatualizados, sistema operacional pirata, firewall[53] desativado, configurações incorretas da rede ou falhas no software, propiciando ataques e danos à máquina e aos seus dados pessoais. Com isso, é de suma importância analisar as formas de ataques, pois diversos são os tipos de pragas cibernéticas que se utilizam diretamente destas falhas para poder invadir o sistema, como exemplos, podemos citar as seguintes:

Malwares é o nome utilizado, para designar programas desenvolvido com o objetivo de causar danos a um computador, sistema ou rede de computadores, proveniente do inglês que significa software malicioso, estes abrangem diversos tipos de ataques, dentre os mais conhecidos podemos citar os vírus, os worms e os cavalos de Tróia. Esses malwares costumam se utilizar de ferramentas de comunicação conhecidas para invadir o sistema, por exemplo, e-mail, mensagens instantâneas e downloads[54]. No mesmo entendimento Spencer Toth Sydow.

> Também denominada inserção de malware, contágio de dispositivo alheio ou sabotagem informática, a conduta é da modalidade de delitos informáticos próprios pu-

[53] **Firewall** é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo.
[54] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 8.

> ros, porquanto a inserção de programas que modificam, alteram ou destroem dados em dispositivos alheios somente pode ocorrer com o uso de telemática[55].

Esses tipos de programas são inseridos nos dispositivos alheios causando-lhes diversos prejuízos, afetando na confidencialidade dos dados, na velocidade dos aparelhos ou até mesmo inutilizando os serviços.

Vale salientar que o objetivo deste trabalho não é esgotar os variados tipos de Malwares, mas sim, apresentar uma breve explanação daqueles que são considerados os que frequentemente acometem os usuários.

São exemplo desta forma de ataque os vírus de computador que são pequenos programas capazes de produzir cópias de si mesmo, hospedando-se em outros programas com o objetivo de infectar arquivos. Porém não podem se auto executar, ou seja, começar a operar sozinho, para começar a agir, estes precisam que alguém ou algo os executem, no entanto têm a habilidade de se replicar em um sistema, podendo assim, se espalhar rapidamente em diversas máquinas, conectadas entre si ou em redes de internet, destruindo arquivos, formatando discos rígidos, parando serviços e mesmo tendo este poder de corromper arquivos e programas o seu objetivo pode ou não está ligado a roubos financeiros ou de informações, caracterizando-se apenas como um vandalismo.

O termo vírus foi usado pela primeira vez pelo pesquisador Frederick Cohen ao denominar os programas de códigos nocivos. Atualmente, professor da universidade de New Haven (Connecticut), afirma que ao produzir o arquivo malicioso tinha o objetivo científico, mas que hoje não faria isso novamente. Na época de sua criação os vírus eram transmitidos principalmente por meio de disquetes, por programadores que queriam demonstrar suas habilidades sem que isso necessariamente implicasse prejuízos as suas vítimas, diferenciando-se assim do que motiva os ataques por vírus na atualidade, pois estes têm objetivo criminoso com grupos organizados por fraudadores[56] como já foi citado.

Outro tipo de ataque são os Cavalos de Tróia. Seguindo a mitologia, estes programas maliciosos procuram se desfaçar para poder penetrar no sistema e fazer suas vítimas. Esses arquivos aparentemente inocentes causam grandes prejuízos ao sistema, pois abre brechas para que no futuro ataques possam ser instaurados. Eles penetram no sistema através de anexos de e-mail ou se encontram disponíveis em sites. O cavalo de Tróia não tem a capacidade de se

[55] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 122.
[56] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 9.

multiplicar, diferenciando-se dos vírus e dos worms, mas se alastram quando as pessoas são tentadas a abrir o programa por pensar que sua origem é uma fonte segura[57].

Outro tipo de programa malicioso que vem causando aborrecimentos aos usuários da rede é o Worm. Software de nome sugestivo, que significa verme em português, é um programa capaz de criar cópias de si mesmo, tornando-se assim independente de outro para agir. Assim como os cavalos de Tróia, estes entram no sistema através de e-mails ou quando o usuário acessa sites onde eles estão presentes.

Os Worms são difíceis de ser detectados, pois não criam arquivos regulares, e muitas vezes só são notados quando começam a afetar o sistema, tornando-o mais lento, ou então, quando atrapalham a execução de outros programas[58].

Para finalizar as formas de ataques mais comuns, que podem vir a acometer o sistema, enquadrados nas falhas técnicas estão os Adwares, são programas que exibem propagandas e anúncios sem a autorização dos usuários, tornando a conexão e o computador mais lento, estes podem baixar uma indesejável barra de ferramentas no navegador do usuário, como também tem a possibilidade de roubar a página inicial do navegador e redirecionar a vítima para outro site, além de causar anomalias no sistema ou incompatibilidades com outros programas[59].

Mesmo este trabalho não estando voltado a se aprofundar no que diz respeito a estes tipos de falhas técnicas, há de se notar que a maioria das pessoas não sabe diferenciar os diversos tipos de programas maliciosos e isso, de certo, influencia nas formas de proteção, pois muitas vezes os usuários do sistema nem sabem, sequer, que a sua máquina está infectada, e como o nosso objetivo é proporcionar o conhecimento acerca do que envolve os delitos cibernéticos, nada mais justo do que trazer, mesmo que de forma sucinta, alguns deles.

Existem várias formas de invadir um sistema e as consequências também são diversas, o objetivo muitas vezes é a simples invasão de computadores alheios com a intenção de danificar os seus componentes, porém a maioria dos ataques visa prejudicar os seus usuários e não apenas a máquina, pois, por traz da invasão, atualmente tem prevalecido a intenção financeira do agente em obter proveito das vítimas.

No gráfico a seguir, podemos verificar a forma como ataques ao ambiente virtual vêm aumentando com o passar dos anos.

---

[57] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 11.
[58] Ibidem, p. 14.
[59] Ibidem, mesma página.

GRÁFICO 3 - Total de incidentes reportados ao CERT.br entre 1999 a 2014.

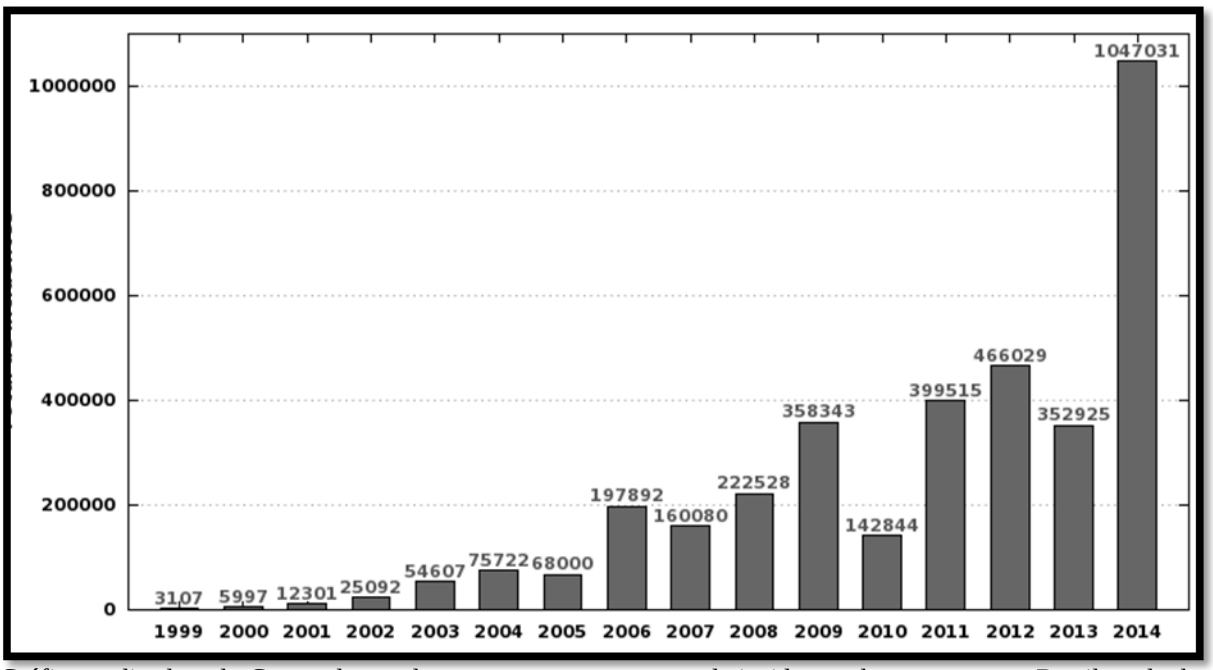


Gráfico realizado pelo Centro de estudos, respostas e tratamento de incidentes de segurança no Brasil, onde demonstra o crescimento dos ataques ao sistema.

Estes dados que foram ilustrados no gráfico acima são o resultado de uma pesquisa realizada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil-CERT.br[60], o mesmo relata de forma clara o assolador crescimento ocorrido entre os anos de 1999 à 2014, tendo alcançado no ano de 2014 quantias estrondosas. Como revela o gráfico, estes incidentes tiveram um padrão de crescimento linear, com pequenas diminuições em períodos específicos, porém, posteriormente retomando o crescimento.

Os usuários do sistema informático, em um curto espaço de tempo, se viram diante de uma tecnologia que está sempre se renovando e muitas vezes não tendo tempo de sequer entender o funcionamento de novos aparelhos que rapidamente são colocados no mercado, com funções mais aprimoradas, isso leva a usuários despreparados que se utilizam do sistema e suportam as falhas de segurança que nele existe, mas as utilidades advindas destes meios, de certa forma, suprem a falta de proteção, restando assim indivíduos despreparados que suportam os riscos em prol das utilidades.

Como exemplo, podemos citar o ataque ocorrido ao DETRAN-PE (Departamento de Trânsito de Pernambuco). Segundo publicação do site G1.Globo, 1.400 computadores foram afetados por um vírus que invadiu o sistema de informação do Departamento Estadual de

[60] **CENTRO DE ESTUDO E RESPOSTA PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL**. Total de incidentes reportado ao CERT.br por ano. Disponível em:<http://www.cert.br/stats/incidentes/>. Acesso em: 06/10/15.

Trânsito de Pernambuco, no início de Fevereiro de 2009, onde o mesmo teve seus procedimentos parados por lentidão e falhas durante requisições de serviços internos, resultando em três dias de serviços e atendimentos paralisados – tempo suficiente para a imprensa estampar as "Matérias de capa" dos jornais. Sabe-se que o worm que causou tamanho prejuízo foi o Conficker (um vírus que tem como objetivo afetar computadores dotados do sistema operacional Microsoft Windows). A forma de infecção em si e o suposto responsável por ela não foram encontrados, porém acredita-se que, algum pen drive infectado tenha sido posto numa máquina interna ao DETRAN-PE. Esta de fato é a versão mais aceita para este tipo de infecção. Segundo especialistas, para o tratamento deste malware, bastavam que os antivírus estivessem num correto funcionamento e os computadores da instituição com uma atualização disponível gratuitamente para sistemas operacionais Windows e todo esse aborrecimento teria sido evitado[61].

Outro exemplo conhecido foi o caso ocorrido no dia 26 de abril de 2014 onde internautas relataram ao portal G1 da Rede Globo, que o acesso a sites, tais como o Google, estavam sendo direcionados para uma página fraudulenta onde continha um download falso do Flash Player[62] que ao ser baixado contaminaria o computador com um vírus. Segundo o site, este incidente já havia ocorrido em 2009 quando a empresa foi vítima de outro ataque semelhante, onde um website de uma instituição financeira foi direcionado para um site clonado roubando informações das vítimas.

Para finalizar vale a pena lembrar que estes ataque e pragas que foram mencionados podem ser minimizados ou até mesmo evitados, para isto faz-se necessário certo cuidado quanto ao ambiente virtual, como já havíamos mencionado anteriormente, pois o mesmo possui suas fragilidades técnicas e humanas, como veremos a seguir, no entanto isso não deve implicar em desleixo por parte dos usuários, tendo os mesmos que assumir sua parcela de responsabilidade, pois ao observarmos os exemplos anteriormente citados reforçamos o entendimento de que apenas tecnologia e processos não são suficientes para garantir a segurança do sistema, porque as falhas verificadas nestes exemplos vão além dos softwares utilizados, sendo as mesmas, por diversas vezes, marcadas por alguma deficiência pessoal.

---

[61] **VÍRUS INTERROMPE SERVIÇO DO DETRAN-PE.** São Paulo: Portal de Notícias G1. 06/02/2009. Disponível em: <http://g1.globo.com/Noticias/Brasil/0,,MUL990097-5598,00-VIRUS+INTERROMPE+SERVICOS+PRESTADOS+PELO+DETRAN+EM+PERNAMBUCO.html>. Acesso em: 01/7/15.

[62] Um reprodutor de multimídia, uma maneira virtual usada para executar arquivos.

2.1.2 Falhas Humanas

O desejo inerente do humano em ganhar algo, em receber bônus e benefícios, muitas vezes é a chave para a entrada em uma situação indesejada e perigosa, com isso, velhos golpes continuam a fazer vítimas, pessoas que são enganadas através de ligações telefônicas, onde são oferecidos brindes, mostrando como a mente humana, muitas vezes está suscetível a enganações. Grande parte das pessoas se engana e não pensam com clareza no brinde inesperado, no e-mail que vai abrir.

A falta de treinamento das pessoas é um problema real, porém negligenciado. Nota-se que é necessário um entendimento das mesmas a respeito do perigo e da prevenção, devendo haver uma conscientização de como pode ser prejudicial clicar em *links* duvidosos, da obrigação de averiguar se o antivírus está atualizado, do perigo de compartilhar senhas, entre outros atos que podem causar riscos. A identificação de um possível comportamento como sendo característico de infecções por vírus ou entender o que as mensagens do antivírus querem dizer é uma ação de fundamental importância para evitar um indesejado problema.

Caminhando junto com a falta de orientação e havendo ou não investimento tecnológico, está a imprudência dos usuários, negligenciando o perigo, pois muitas precauções poderiam ser tomadas simplesmente com a aderência de boas práticas de utilização, tendo em vista que alguns erros são básicos e recorrentes. Podemos mencionar algumas práticas cometidas por usuários que se fossem mais bem analisadas ou se houvesse uma devida proteção poderiam não ser tão danosas; como por exemplo: clicar em links maliciosos, pois muitas vezes as pessoas imaginam o sistema de defesa como sendo algo infalível pelo simples fato de possuir um antivírus ou firewall, com isso clicam em links sem maiores critérios achando que não ocorrerão grandes problemas.

Outro problema comum é a forma como as pessoas cuidam das suas senhas, pois estas são a identificação pessoal de cada usuário, as informações acessadas através delas dizem respeito exclusivamente àquela pessoal e a vincula ao sistema. É a partir da falta de cuidado, compartilhamento ou negligencia das mesmas que muitas vezes acabam “autorizando” a utilização de serviços que apenas com uma identificação pessoal seriam possíveis e possibilitando que um terceiro, alguém que não é o real proprietário da senha, a utilize, podendo muitas vezes usar de má-fé. Essas senhas por muitas vezes são fracas ou até mesmo o usuário pode repetir a mesma, utilizando-se de uma senha única para várias ações e serviços diferentes, sendo esse um ato arriscado, pois quando fracas, podem ser facilmente descobertas, e atualmente já

existem programas voltados exclusivamente para essa finalidade, por esse motivo a necessidade de se criar senhas mais elaboradas.

Em países mais evoluídos, o tema sobre segurança no mundo virtual começa desde pequeno, como matéria de sala de aula ou mesmo em forma de palestras e grupos de discussão, seguindo esse exemplo, deve-se ser lembrado que se hoje a internet já é fundamental no nosso cotidiano, daqui a alguns anos ela será indispensável e todos estarão conectados a ela. Assim, ensinar a lidar com a internet e seus males precisa começar na infância, seja na escola ou em casa, e os adultos precisam se reeducar, precisam estar sempre atentos aos acontecimentos e aos contatos e atos que acabam tendo e cometendo na rede.

Finalizando nossa análise sobre diversas formas de ataques, voltamos a mencionar dados da Pesquisa Nacional de Segurança da Informação realizada em 2014 pela empresa Daryus. Neste gráfico estão expressos os diversos problemas e os incidentes mais frequentes foram destacados[63].

GRÁFICO 4 - Incidentes mais Frequentes.

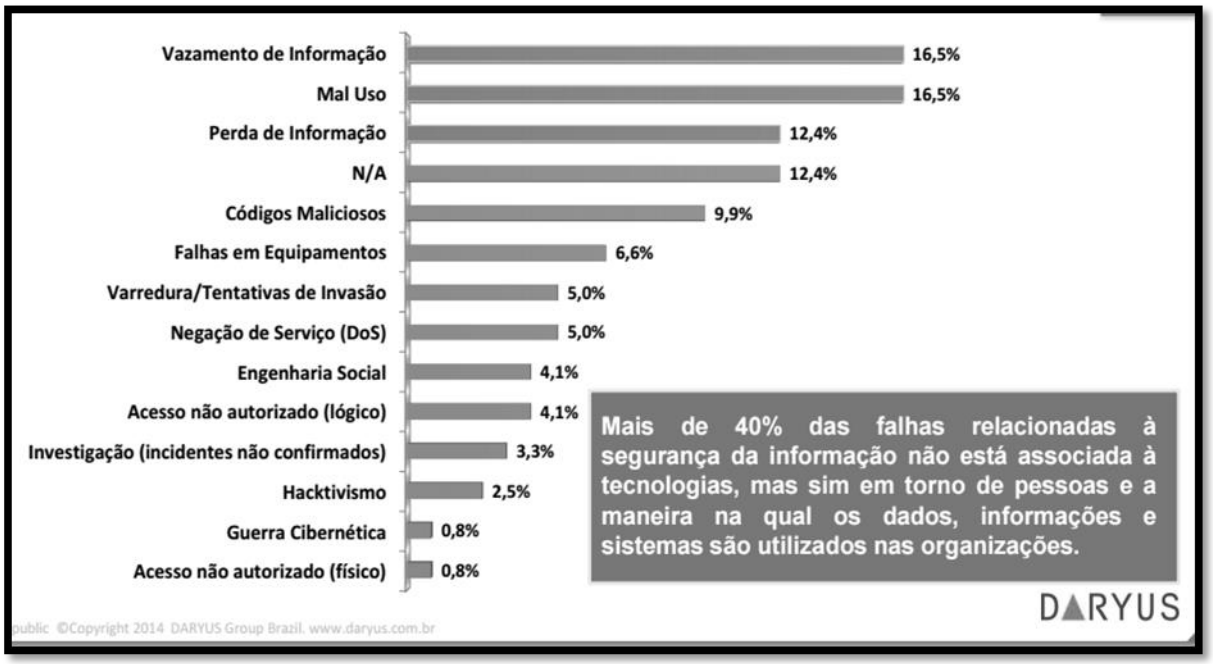


Gráfico da Pesquisa Nacional de Segurança da Informação, publicado em 2014, realizada pela empresa Daryus, que retrata os incidentes mais frequentes envolvendo segurança da informação.

Vemos que a segurança das informações depende da tecnologia, dos processos e das pessoas, e infelizmente, o problema não está apenas na parte técnica, que muitas vezes dribla-

[63] **PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO REALIZADA EM 2014 POR A EMPRESA DARYUS**. DARYUS Group Brazil: Public Copyright 2014. Disponível em: < http://www.daryus.com.br/view/pdf/DARYUS_Pesquisa_ISM.pdf>. Acesso em: 13/07/2015.

da pelo constante surgimento de novas ameaças, faz com que o perigo venha a sucumbir o sistema, mas também o problema é proveniente das falhas humanas, pois esta é considerada "a parte mais frágil". Segundo publicação no ano de 2014 da Pesquisa Nacional de Segurança da Informação, ao ser analisado os maiores causadores de falhas de segurança, as pessoas são vistas como sendo grandes responsáveis por incidentes, representando aproximadamente 16,5% das ocorrências por mau uso e vazamento de informações[64]. Essa participação humana pode acontecer de forma direta ou indireta, com intenção ou sem, pois de início as pessoas costumam confundir a proteção do espaço físico das máquinas com a segurança das informações em si. As pessoas que falharam, são as mesmas que usam os recursos tecnológicos, e a tecnologia sem a correta utilização torna-se algo arriscado para o próprio usuário e para terceiros.

São exemplos comuns de falhas humanas clicar em *links* suspeitos, escrever senhas em bilhetes colados à máquina, sucumbir a um pedido mais gentil de informações, é aí onde entra a figura da Engenharia social[65]. Embora se tenha dado um grande avanço no sentido de criar sistemas computacionais cada vez mais seguros, isso pode de nada valer frente à engenharia social, que consistem em técnicas para convencer o usuário a entregar dados como senhas bancárias, número do cartão de crédito, dados financeiros em geral, seja numa conversa informal e despreocupada em uma sala de bate papo, em um messenger, onde geralmente costumam ocorrer tais atos, e até mesmo pessoalmente, por isso, nunca se deve fornecer qualquer tipo de senha, pois esta é a porta de entrada para o acesso a informações, espionagem, furto de dinheiro em conta bancária e detalhes pessoais, podendo cair nas mãos de pessoas desconhecidas que não se sabe o tipo de destino que podem dar a esses elementos.

Engenharia Social é uma forma muito utilizada na prática do crime cibernético, nela quase não se emprega meios digitais, pois o seu foco se dará sobre o fator humano, como já foi citado anteriormente, os programas de computadores servem apenas de complementos e em outras vezes não são sequer utilizados, pois sua principal característica é o poder de persuasão. São pessoas que buscam extrair informações das mais diferentes formas, como por exemplo, fazendo ligações telefônicas, especulações e espionagens. Como menciona Oliveira Cassanti.

---

[64] **PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO REALIZADA EM 2014 POR A EMPRESA DARYUS**. DARYUS Group Brazil: Public Copyright 2014. Disponível em: < http://www.daryus.com.br/view/pdf/DARYUS_Pesquisa_ISM.pdf>. Acesso em: 13/07/2015.

[65] MITNICK, Kevin D.; SIMON, William L. **A arte de enganar – Ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Education, 2003. p. 33.

> Esta prática visa à enganação ou exploração da confiança dos usuários levando-os a efetuar uma determinada ação para obter informações importantes ou sigilosas sobre eles. Geralmente o golpista se faz passar por outra pessoa ou instituição, ou fingir ser um profissional em determinada área.
> A diferença entre ataques de engenharia social e, por exemplo, a tentativa de um atacante conseguir acesso a um determinado site é a escolha das ferramentas utilizadas. Um atacante irá procurar por vulnerabilidade no serviço da vítima enquanto um engenheiro social utilizará algumas técnicas de persuasão estimulando o medo, a curiosidade, a ganância ou a simpatia da vítima para obter a informação ou acesso desejado[66].

O Engenheiro Social prevê a suspeita e a resistência, e ele está sempre preparado para transformar a desconfiança em confiança e quanto mais os especialistas evoluem na sua tecnologia com a segurança, tornando mais dificultoso a exploração da vulnerabilidade técnica, os ataques visarão, cada vez mais, o elemento humano, enganando, influenciando ou manipulando para revelar informações ou executar ações. O ser humano não foi treinado para suspeitar uns dos outros e sendo assim, se deixa levar pela curiosidade, acredita na sorte de que "não irá acontecer com ele", e na boa-fé, por motivos como estes é que sempre está em ascensão está modalidade de crime, na sua forma originária, com um delito que existe por intermédio da tecnologia ou como uma maneira qualificada de um crime já existente, como veremos a seguir, ambas as formas atingem de maneira significativa a vida de quem utiliza o meio virtual, merecendo uma especial atenção não apenas por parte dos usuários e provedores, mas também dos Operadores do Direito, visto que esta é uma das principais formas de criminalidade no futuro.

2.2 Tipos de Crimes Cibernéticos

Tendo em vista o constante crescimento tecnológico faz-se necessário enfatizar a dificuldade de se mencionar todos os crimes que podem ser executado por intermédio do ambiente virtual, sendo assim, os delitos que serão mencionados a seguir, trata-se de condutas já tipificadas no Código Penal, tendo na sua execução por meios virtuais uma forma qualificada, por assim dizer. No ambiente virtual a possibilidade delitiva se desenvolve dia após dia, e com isso, novas formas vão surgindo de praticar os mesmos, ou um novo delito, por esse motivo tornar-se-ia custoso o alistamento de todas as formas de crimes virtuais.

Devemos deixar bem claro que o objetivo central do nosso trabalho não está voltado a descrever os tipos de crimes cibernéticos, mas sim, trazer uma contribuição acerca das formas de proteção e como as pessoas podem agir caso venham a ser vítima desses delitos, porém de

[66] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p.15.

suma importância será a menção de alguns deles, tendo em vista que difícil seria falar em crimes cibernéticos sem que houvesse essa análise, outro ponto de imprescindível destaque será abordado no terceiro capítulo, este tratará do Ordenamento Jurídico Brasileiro no que concerne a regulamentação do ambiente virtual, nele falaremos do Marco Civil da Internet, que apesar de tratar-se de uma Lei Civil, está será de essencial importância ao analisar assuntos relacionados ao ambiente virtual, e da Lei nº 12.737/12, ao regular o tema no Código Penal.

Como já foi mencionado anteriormente, os crimes cibernéticos não são praticados apenas por pessoas com conhecimento sofisticado de informática, as redes sociais como Facebook, Twitter, YouTube, são instrumentos comumente utilizados na prática de delitos como, calúnia, desrespeito por motivo de cor, etnia ou opção religiosa. O maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem lei, por isso, muitas vezes os autores acreditam que suas ações ficaram impunes.

A lista de crimes que podem ser cometidos por meio eletrônico é extensa, porém, na maioria dos casos é possível fazer uma adaptação à legislação vigente. Para o judiciário, 95% dos delitos cometidos eletronicamente já se encontram tipificados no Código Penal Brasileiro, ou seja, caracterizando-se crimes comuns praticados através da internet, enquanto os outro 5%, para os quais falta enquadramento jurídico, trata-se das transgressões que só existem no mundo virtual como, por exemplo, as distribuições de vírus eletrônicos[67].Veremos a seguir essas distinções.

2.2.1 Crimes Contra o Patrimônio

Diversos são os crimes contra o patrimônio que podem ser praticados pela internet, podendo ter como vítima tanto pessoa física quanto jurídica. O patrimônio não se limita apenas a bens corpóreos como também incorpóreos de valores pecuniários ou de valores sentimentais, ou seja, não se restringindo apenas ao que é aferível economicamente.

Dentre os mais cometidos podemos citar os crimes de: Estelionato; Dano; e Furto, que são espécies de crimes que tem o meio virtual como sendo um novo aliado na sua prática. O estelionato é um dos crimes mais populares, tanto na internet, quanto fora dela, e sua conduta varia conforme o agente faz uso dos meios eletrônicos disponíveis. Está descrito no Código Penal em seu art. 171, *caput*, dito que: "art. 171. Obter, para si ou para outrem, vantagem ilí-

[67] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 24.

cita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa".

No caso do estelionato praticado por meios eletrônicos não é diferente, pois o agente tem como objetivo induzir ou manter a vítima em erro para com isso obter para si ou para outrem vantagens ilícitas causando assim prejuízo às vítimas. No entanto são inúmeras as condutas que podem ser tipificadas como estelionato cometido na internet, sendo em sua maioria fraudes que procuram conseguir o consentimento das vítimas, iludindo-as para que voluntariamente entreguem o bem, pratiquem o ato que permite a concretização desses crimes.

Quanto ao sujeito ativo do estelionatário virtual, trata-se de pessoas que tenham certo conhecimento de informática, pois, cada vez mais ardilosos e engenhosos são os delitos praticados nessa área. Já o sujeito passivo será qualquer pessoa capaz, porém pode o sujeito passivo, ser diverso da pessoa enganada, ou seja, no caso de se enganar alguém para que através dessa pessoa possa se atingir o patrimônio de terceiro.

Difícil é a tipificação das condutas dos estelionatários na internet, uma vez que elas são diversas, dificultando o seu enquadramento. Um exemplo de estelionato aplicado atualmente trata-se do ato de enviar e-mails com conteúdo falso aos usuários com o objetivo obter informações referentes a contas bancárias, dados pessoais como RG e CPF ou informações referentes à empresa onde o usuário trabalha, entre outras informações de crucial importância. O golpe se concretiza no momento em que o usuário clica no *link* do corpo do e-mail e é direcionado para um *site* onde os seus dados são utilizados maliciosamente.

Segundo a notícia do *site* G1do dia 12 de maio de 2015[68], Outro caso que tem sido preocupante diz respeito a um novo golpe, popularmente chamado de "golpe do boleto" onde o estelionatário através de e-mails ou links falsos introduz programas maliciosos no sistema operacional do aparelho do usuário, esses programas substituem dados nos boletos que serão gerados pelo usuário fazendo com que o número da conta, impressa no código de barras, seja alterado e substituído por o número de uma conta do agente, com isso a vítima ao pagar o boleto, terá os valores depositados na conta do estelionatário e não na conta da empresa que a vítima realmente tem a dívida.

Dito isto, vejamos o entendimento de um jurisprudencial tribunal de Justiça do Rio Grande do Sul.

---

[68] **GOLPE DO BOLETO FALSO NA INTERNET FAZ CADA VEZ MAIS VÍTIMAS NO PAÍS**. Disponível em:<http://g1.globo.com/jornal-nacional/noticia/2015/05/golpe-do-boleto-falso-na-internet-faz-cada-vez-mais-vitimas-no-pais.html>. Acesso em: 25/08/15.

> **RECURSO INOMINADO. AÇÃO DE REPARAÇÃO DE DANOS. FRAUDE EM SEGUNDA VIA DE BOLETO BANCÁRIO. PAGAMENTO DESVIADO PARA TERCEIRO. ILEGITIMIDADE PASSIVA AFASTADA. DANO MATERIAL COMPROVADO. DANO MORAL NÃO CONFIGURADO.** Afastada a ilegitimidade passiva da cooperativa ré. Restou incontroversa a fraude perpetrada através dos serviços bancários prestados pela demandada. Aplicação do parágrafo único do art. 927 do CC e da Súmula 479 do STJ. Legitimidade da ré para responder frente aos prejuízos suportados pela demandante. Análise do mérito com base no permissivo do art. 515, § 3º do CPC. Devidamente comprovados os fatos constitutivos do direito da parte autora. A narrativa inicial é corroborada pelos documentos juntados, ou seja, o boleto fraudado devidamente quitado, e as faturas telefônicas indicando a tentativa de solução administrativa da questão (Art. 333, I do CPC). A responsabilidade da ré está configurada à medida que a fraude se tornou incontroversa. Esta ainda esclareceu o modo pelo qual o golpe foi operado. Assim, deve indenizar a autora. Dano material comprovado em parte, mediante a juntada aos autos do boleto fraudado devidamente quitado pela demandante. Ausência de comprovação dos gastos com ligações telefônicas, de maneira que não merecem guarida. Embora as faturas indiquem a realização das ligações, não há no feito comprovante de seu efetivo pagamento, pelo que não pode haver ressarcimento. Dano moral não configurado. Meros dissabores enfrentados diante da situação. Ausência de afronta aos atributos de personalidade da autora que conduz, inevitavelmente, ao não reconhecimento do instituto. RECURSO PROVIDO EM PARTE SENTENÇA REFORMADA (Recurso Cível Nº 71005058870, Segunda Turma Recursal Cível, Turmas Recursais, Relator: Ana Cláudia Cachapuz Silva Raabe, Julgado em 24/09/2014)
> (TJ-RS - Recurso Cível: 71005058870 RS , Relator: Ana Cláudia Cachapuz Silva Raabe, Data de Julgamento: 24/09/2014, Segunda Turma Recursal Cível, Data de Publicação: Diário da Justiça do dia 29/09/2014)
> (TRF-3 - RSE: 7720 SP 2010.61.02.007720-3, Relator: DESEMBARGADOR FEDERAL COTRIM GUIMARÃES, Data de Julgamento: 16/08/2011, SEGUNDA TURMA)[69].

A consumação do estelionato, em sua modalidade básica acontece com o êxito do agente ao conseguir vantagens de forma ilícita sobre o patrimônio da vítima, já o que caracteriza o estelionato nos crimes cibernéticos é o meio ardil, fraudulento ou artificioso que é usado pelo estelionatário para alcançar o patrimônio da vítima.

Quanto ao delito de dano, quando praticado através da rede, um dos mecanismos que dá causa a sua propagação é a disseminação dos vírus e o bem jurídico penalmente tutelado é o patrimônio, que deve ser entendido como conjunto de bens de valor econômico ou afetivo para seu proprietário. Ele está previsto no art. 163 do Código Penal Brasileiro e este é aplicável á tutela dos dados informáticos, pois se trata de interpretação extensiva da palavra "coisa", elemento objetivo do tipo penal.

A proteção patrimonial dos dados não se limita a seu valor econômico, pois a intenção é proteger todo patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor afetivo que porventura tenha a coisa, sendo assim, se a ví-

[69] BRASIL. **Tribunal de Justiça do Rio Grande do Sul**. Recurso Cível n°71005058870/RS. Relator: CACHAPUZ, Ana Cláudia, Publicado no DJ de 29/09/2014. Disponível em:<http://tj-rs.jusbrasil.com.br/jurisprudencia/142667010/recurso-civel-71005058870-rs>. Acesso em: 14/10/15.

tima tem armazenado em formato digital algum documento, e-mails, fotografias ou algo que possua ou não valor econômico, certamente esses arquivos podem ser objeto do crime de dano.

Seguindo nesta linha de pensamento, é conveniente expor que, majoritariamente, o objeto do crime de dano visa à coisa móvel ou imóvel, sendo por óbvio uma coisa corpórea no sentido realístico, pois somente essa pode ser danificada por ação física. Logo, para o dano virtual bastaria o ataque ou destruição de arquivos; informações; dados ou até um vírus que acarrete a quebra do corpo físico de um computador, mesmo que não tenham valor econômico, pois, o mesmo pode ter um significado ao seu detentor. Quanto ao dado que possua valor econômico é inquestionável atribuí-lo, quando lesado, a figura do dano virtual.

Vale lembrar ainda que, se a coisa tiver valor econômico, este deve ser significativo, pois caso contrário aplicar-se-ia o princípio da insignificância que exclui a própria tipicidade. Os vírus informáticos, por sua vez são grandes causadores de danos a seus hospedeiros, em regra o sistema operacional de um computador. A divulgação de vírus informáticos, com intenção de dano, pode ser punida como tentativa de dano, caso o resultado não se concretize ou como dano consumado, caso o resultado naturalístico venha a ocorrer efetivamente. Esse tipo de crime consuma-se no momento do resultado, porém no caso de dano causado por vírus de computador, esse resultado apenas ocorrerá depois, podendo ou não levar muito tempo.

Outro crime que está em ascensão é a fraude praticada por meio da internet, por ser esse meio um dos mais utilizados na compra e venda de mercadorias e operações financeiras, um constante aparecimento de companhias e indivíduos oferecendo produtos e serviços através dela tem sido notório. O problema é que com a mesma rapidez que essas práticas estão virando um habito uma comodidade, também estão aumentando a quantidade de indivíduos maliciosos, aproveitando-se de um suposto anonimato para enganar os usuários.

Por esse motivo o delito de fraude tem tomado um novo formato, porém com um mesmo objetivo, tirar proveito das vítimas, como por exemplo, em uma operação de compra e venda por intermédio da internet quando essa mercadoria nunca chega ao seu destinatário ou ainda quando o produto chega ao destinatário, mas não condiz com a imagem publicada no site[70]. Outro fato preocupante diz respeito às formas de pagamento que em sua maioria são efetuados via cartão de crédito por oferecer uma maior comodidade as seus usuários, fato este que faz com que os usuários esqueçam o perigo, pois ao se efetuar um pagamento, via inter-

[70] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 50. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

net, utilizando-se de cartão de credito, esse usuário tem os seus dados pessoais e do cartão gravados automaticamente no sistema do site onde essa pessoa fez a operação financeira.

Vale lembrar que a fraude quanto ao cartão não se limita à relação cliente-comerciante, sendo possível que a transação seja interceptada e uma terceira pessoa, mal intencionada, venha a ter acesso às informações ali contidas, ou seja, não são apenas os provedores que transmitem quanto os que recebem informações que têm acesso aos dados de cartões de crédito, podendo utiliza-los ilegalmente interceptando tais informações, qualquer pessoa que tenha as ferramentas e o conhecimento apropriado para tanto também pode.

2.2.2 Crimes Contra a Honra

São crimes que se propagam rapidamente e com o uso da internet se tornaram mais comuns, com ilustrações como vídeo, foto, mensagens com áudio, criação de blogs, sites de relacionamento dentre outras maneiras de ofender e ser ofendido, seja direta ou indiretamente que acabou se tornando rotina na vida de quem acessa a grande rede. São crimes que mesmo cometidos pela Internet, devem ser denunciados pela vítima na delegacia mais próxima ou em uma delegacia especializada em crimes cibernéticos, pois se trata de crimes de ação privada, ou seja, que dependem de representação.

Nesta classe podemos mencionar os crimes de Calúnia[71], previsto no artigo 138 do Código Penal Brasileiro, onde a vítima é acusada falsamente por alguém da prática de fato definido como crime, colocando em dúvida a sua credibilidade no meio social, ou seja, o autor divulga falsamente a informação caluniosa, devendo, para isso existir na sua informação divulgada uma imputação criminosa à vítima com a devida correspondência legal para que possa ser enquadrado nesse crime. Porém, para tanto, é necessário a intenção prejudicial, pois não havendo intenção de informar dado falso não será constituído com tal crime. Sendo assim, vale deixar claro que Calúnia só existe quando houver divulgação, logo é necessário que a falsa afirmação chegue ao conhecimento de uma pessoa que não seja o ofendido. Se, por exemplo, for um e-mail ou mensagem eletrônica de conteúdo visto apenas pelas partes não tratar-se-á de calúnia.

Diferente da Calúnia, o Código Penal brasileiro, no seu artigo 139 tratará da Difamação[72], pois é mais um dos crimes contra a honra que pode ser praticado via internet. Consiste em atacar a reputação de alguém diante à sociedade, atribuindo-lhe fato ofensivo, e não ape-

[71] GRECO, Rogério. **Código Penal Comentado**. 4. ed. Niterói: Impetus, 2010. p. 311.
[72] Ibidem, p.321.

nas negativo ou inconveniente, trata esse dispositivo legal da honra objetiva, da imagem social da vítima. Na Difamação a lei não exige que a atribuição seja falsa, basta somente à perpetuação de algo que venha a ofender a reputação do agente perante a sociedade e mais uma vez entra a publicidade dada através da internet nesse ato ofensivo. Uma dificuldade encontrada nesse tipo de crime diz respeito à certificação se realmente houve a ofensa, pois em muitos casos existe a possibilidade da intenção do agente não ser de ofender, mas sim uma forma habitual de se expressar.

Quanto ao crime de injúria consiste na propagação de qualidade negativa da vítima por um terceiro, qualidade esta que diga respeito aos seus atributos morais, intelectuais ou físicos, ofendendo, insultando e com isso atingindo a dignidade ou a moral de alguém, afetando de forma significativa a honra subjetiva da vítima, ou seja, o conceito que cada um tem de si próprio. Ressalve-se que mesmo essas qualidades negativas atribuídas pelo agente à vítima sendo verdadeiro, o sentido injurioso das atribuições permanecem. O tipo penal está previsto no art. 140 do Código Penal.

Na injúria não há imputação de fato, mas sim de qualidade negativa à vítima, o que torna extremamente dificultoso o seu enquadramento ao elemento essencial do tipo do crime, ficando muito complexa a distinção entre brincadeira e real imputação de injúria, porém não se deve confundir com o crime de racismo, pois este último configura-se quando o agente pretende, com o ato, impedir ou dificultar o acesso de alguém a algo, ocasionando com isso uma segregação racial, já a injúria ocorre quando, por exemplo, nas redes sociais o injuriador se utiliza do fato da vítima ser negra para fazer disto um insulto, como se essa condição configurasse uma qualidade negativa. Segundo Moisés de Oliveira Cassanti.

> Vítimas que tiverem fotos ou vídeos íntimos divulgados têm seus casos analisados através do artigo de crimes contra a honra: como difamação (o ato de disponibilizar imagens íntimas de uma pessoa) ou injúria (ofensas realizadas em meio digital). Mesmo que a pessoa tenha admitido que seu parceiro tirasse as fotos, não é permitido que tais imagens sejam repassadas. Portanto, quem tiver a integridade manchada na internet possui total respaldo judicial[73].

Em ambiente virtual, quaisquer dos crimes contra a honra, irão se consumar, por exemplo, quando alguém espalhar algo sobre uma pessoa pelas redes sociais, e os usuários presentes fizerem a leitura, tomando conhecimento do fato que macula a reputação da vítima, podendo ocorrer em *chats, blogs, redes sociais*, através de publicações em *homepages*, entre outros. Seus agentes são incentivados pelo anonimato (lembrando que o anonimato é vedado pela Constituição Federal em seu artigo 5°, inciso IV) e pela dificuldade que há na investiga-

[73] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 59.

ção quando se trata de crimes cometidos via internet. Essas formas de conduta criminosa contam com o agravante do inciso III do art. 141 do Código Penal, por conta da divulgação, ou seja, da publicidade proporcionada pela internet.

2.2.3 Crimes Contra a Dignidade Sexual

Ao falar de crimes contra a dignidade Sexual nos remetemos ao Código Penal, Parte especial, onde estão elencados os crimes de favorecimento à prostituição no artigo 228, de escrito ou objeto obsceno no artigo 234 e na Lei nº 8.069/90 no seu artigo 240 o crime de pornografia infantil. No crime de favorecimento à prostituição, devemos lembrar que a prostituição é uma das profissões mais antigas da humanidade e ela em si é considerada uma conduta indiferente ao Direito Penal, ou seja, é um fato atípico[74]. O I Congresso Mundial contra a Exploração Sexual de Crianças e Adolescentes, realizado em Estocolmo no ano de 1996, apontou como sendo a prostituição uma das modalidades de exploração sexual, juntamente com o turismo sexual, a pornografia e o tráfico para fins sexuais[75].

A *internet* foi um fator crucial no aumento da oferta de serviços sexuais, com o desenvolvimento da tecnologia e dos meios de comunicação se diversificou o comércio do sexo, alargando-se a indústria pornográfica e de seus objetos obscenos[76], hoje é muito comum encontrar *sites* de pornografia e de prostituição, aliás, é muito difícil fazer uma pesquisa em um *site* de busca, sobre qualquer tema, em que não apareça pelo menos um resultado indicando um *link* sobre pornografia.

A *internet* constitui-se no mais moderno meio de comunicação e historicamente falando todos os meios de comunicação foram utilizados para a difusão da pornografa. Por exemplo, com a invenção da câmara fotográfica foram encontradas fotos de jovens prostitutas em poses obscenas como sendo algo comumente fotografado pelo então novo equipamento, como também nos anos de surgimento da internet, mesmo sendo objeto de uso quase que exclusivo de universidades, era possível encontrar *sites* de discursões sobre sexo explícito e imagens obscenas[77].

---

[74] GRECO, Rogério. **Código Penal Comentado**. 4. ed. Niterói: Impetus, 2010. p. 644.
[75] Ibidem, p. 645.
[76] Vale lembrar que o conceito de obsceno hoje não é mais o mesmo da inspiração do legislador do Código Penal de 1940.
[77] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 44. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

A pornografia infantil é uma das práticas mais preocupantes para o ordenamento jurídico, esse ato vai desde materiais obscenos envolvendo crianças e adolescente até fotos de mutilações e rituais macabros[78]tendo na internet um terreno fértil para esse crime, porém da mesma forma como é crescente a prática da pornografia infantil na rede de computadores, também está sendo o seu combate, pois a legislação pátria penal prevê punição rígida para os agentes desse ato. O artigo 241 do Estatuto da Criança e do Adolescente reza que é crime "fotografar e publicar cenas de sexo explicitou ou pornografia envolvendo crianças e adolescentes", no mesmo entendimento o STF, desde Setembro de 1998, indicou que o mesmo artigo tem aplicação para atos perpetrados pela internet[79].

Segundo notícia no site G1 do dia 02 de novembro de 2015, a Polícia Federal, deflagrou no Rio Grande do Norte a operação que chamaram de Gênesis, com o objetivo de combater o armazenamento e a distribuição de fotos e vídeos de material pornográfico infantil pela internet. Em Brasília, as investigações a respeito da prática no Estado foram iniciadas há oito meses por meio de um trabalho de inteligência, onde identificaram contas de usuários que se utilizavam de redes sociais e de e-mails para distribuir arquivos de pornografia infantil através da rede mundial de computadores[80].

Importante destacar que esta obra não tem como objetivo elencar todos os crimes cibernéticos, pois bem sei que isso seria um trabalho não apenas para uma única obra, tendo em vista que os delitos cometidos com intermédio da tecnologia são diversos e que vem sempre crescendo, dentre os que não foram mencionados podemos citar a lavagem de dinheiro, roubo através de transferências eletrônicas, contrabando, terrorismo, invasão de privacidade, violação à propriedade intelectual e industrial, espionagem, pirataria, tráfico internacional de armas, jogos ilegais, entre outros[81] que não mencionaremos aqui. Porém, apesar de todo esse avanço delitivo, devemos ressaltar que o combate aos crimes cibernéticos têm sido crescente no Brasil e no Mundo, mesmo tratando-se de práticas já existente, faz-se importante lembrar que são formas novas de agir, dificultando a investigação e persecução penal desses delitos, porém é de suma importância lembrar que muitos dos crimes descritos acima necessitam do

---

[78] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 45. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

[79] ARAS, Vladimir. **Internet Legal: O Direito na Tecnologia da Informação**. 1. ed. Org. Omar Kaminski. Curitiba: Juruá, 2011. p. 119.

[80] **COMBATE A PORNOGRAFIA INFANTIL CUMPRE MANDADOS EM 3 CIDADES**. Disponível em:<http://g1.globo.com/rn/rio-grande-do-norte/noticia/2015/09/combate-pornografia-infantil-cumpre-mandados-em-3-cidades-do-rn.html>. Acesso em: 05/09/15.

[81] SILVA, Mauro Marcelo de Lima. **Internet Legal: O Direito na Tecnologia da Informação**. 1. ed. Org. Omar Kaminski. Curitiba: Juruá, 2011. p. 30.

auxilio das vítimas para que haja a devida investigação e punição, pois no Brasil, a queixa crime ainda é uma prática pouco exercida pelos cidadãos, dificultando com isso a devida punição dos culpados e não condizendo os quadros estatísticos com a realidade, pois sabido é que existem mais práticas de crimes virtuais do que realmente é apurado pelos órgãos competentes.

2.3 O Perfil da Vítima e do Autor

Os computadores de mesa, aparelhos celulares smartphones, tablets e notebooks (netbooks e ultrabooks), são atualmente os equipamentos eletrônicos mais utilizados na prática de condutas reprováveis, porém para que haja a aquisição destas máquinas se faz necessário algum poder aquisitivo e a depender da espécie do delito informático, será necessário algum conhecimento técnico para que seja possível a consumação, esta qualificação técnica vai desde básica até um conhecimento amplo e complexo. Quanto ao sujeito ativo, diferentemente da crença popular, também pode ser um indivíduo comum, não precisando necessariamente ser um expert [82]em informática, pois muitos desses delitos, como por exemplo, os cometidos contra a honra podem até mesmo ser praticados por pessoas que mal dominam a escrita, fato este que tem comumente acontecido por conta da proliferação das redes sociais, outro fator contributivo para a prática do crime cibernético diz respeito ao aumento das oportunidades e um baixo risco de identificação de quem os pratica.

Com o tempo comprovou-se que o perfil dos criminosos são diversos[83], dependendo da natureza dos delitos cometidos, ou seja, uma pessoa que desvia dinheiro de uma instituição financeira é muito diferente do criminoso que comercializa imagens pornográficas de menores. É evidente que, atualmente, qualquer pessoa pode figurar como sujeito ativo do crime cibernético, pois na própria internet serão encontrados inúmeros *sites* que orientam qualquer indivíduo a praticar o crime, trata-se de fóruns, nos quais se ensinam detalhadamente como agir para usurpar senhas de redes sociais, ou até mesmo como criar vírus, ou de conteúdo impróprio, como nos casos de pornografia infantil, com toda essa facilidade na busca de informações e com a sensação cada vez mais clara de total anonimato, pessoas comuns cometem atos ilícitos seja para denegrir a imagem de algum desafeto, seja para fazer uma brincadeira de mau gosto com algum amigo. Passou-se o tempo em que o agente de crimes cibernéticos era

[82]Termo que significa perito ou especialista; pessoa cujo conhecimento excessivo a faz entender ou dominar certa área, assunto, ofício, atividade etc.
[83] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2. ed. São Paulo: Atlas, 2011. p. 40.

um perito em operações de computadores e sistemas eletrônicos, atualmente com as facilidades ocasionadas pelo desenvolvimento tecnológico e com as inúmeras informações da própria rede, qualquer indivíduo poderá tornar-se um criminoso eletrônico, bastando para isso possuir a mínima noção de como operar um computador ou smartphone, assim tornando-se um criminoso em potencial.

Ao contrário do que era necessário em meados do século XX, quando surgiram os delitos cibernéticos, onde os agentes eram vistos com um perfil específico, possuidores de conhecimento técnico detalhado, estes chegando a ser contratados por empresas de grande porte após o término de suas penas, hoje o crime de internet enquadra-se na categoria de crimes de oportunidade, onde o autor se aproveita de uma ocasião propícia para praticar o delito, mas muitos destes agentes não possuem uma personalidade criminosa, mas sim um indivíduo que se aproveita da oportunidade e facilidade para praticar um ato ilícito, segurando-se na ideia do anonimato e no distanciamento que o ambiente cibernético proporciona. Muitas vezes, trata-se de profissionais que laboram na área da informática e praticam o delito contra os seus empregadores, porém isso não implica que pessoas de outra área possam vir a praticar[84].

Diferente do perfil que durante algum tempo foi passado pela mídia, de um indivíduo jovem, do sexo masculino, avesso à violência, com boa aparência, de classe social elevada e possuidor de inteligência acima da média, quem pratica esse tipo de crime na atualidade, são pessoas não tão jovens, podendo ou não estar trabalhando com algo ligado à informática e dependendo do delito que será praticado, não se exigindo um grau de inteligência tão alto, sendo estes, possuidores de algumas características ímpares, como por exemplo, o desrespeito ao Estado e as coisas públicas, sem falar na falta de pudor social[85].

Ao se analisar o sujeito passivo do crime de internet, podemos constatar que pode ser tanto pessoa física ou jurídica, de natureza pública ou privada, pode ser vítimas indivíduos, instituições creditícias, governos e outras, conectadas ou não a internet. O sujeito passivo do crime é o titular do bem lesado ou ameaçado pela conduta criminosa, nada impede que em um delito dois ou mais sujeitos passivos existam desde que tenham sido lesados ou ameaçados a seus bens jurídicos.

Muitas vezes, essas vítimas, além de ser prejudicadas no seu bem ou na sua honra, também o são por sua falta de conhecimento, tanto no que diz respeito à máquina quanto ao que tange os seus direitos. No que concerne às máquinas, nem sempre a pessoa afetada pelo delito perceberá de imediato que foi vítima de tal, ou seja, por não saber lidar com novas tec-

[84] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. pp. 141-148.
[85] Ibidem, pp. 142-145.

nologias, tardará a perceber a real gravidade do problema, quando por fim se é percebido, muitas vezes por constrangimento ou falta de informação a respeito dos seus direitos, faz com que não procurem uma solução, deixando de lado o problema[86].

Uma vez que os delitos informáticos poder ser tidos como uma nova forma de se praticar velhos delitos, uma ferramenta, ou como ações novas que violam bens jurídicos antigos, é fundamental que se aceite o fato de que há certas características particulares da vítima possíveis de influenciar na possibilidade do crime, visto isto, o próprio Código Penal em seu artigo 61 criou uma lista de vítimas consideradas especialmente distintas e sua ofensa leva a um agravamento na pena[87].

Há vítimas que incitam o delinquente a cometer as infrações, agindo estas de forma direta ou indireta. A provocação indireta ocorre por ações negligentes ou imprudentes que favorecem a prática delitual. Já a provocação direta ocorre quando a vítima age com um verdadeiro dolo ao contribuir para que haja o delito contra si ou contra outrem.

Traremos agora, um rol exemplificativo de modalidades vitimaria impactantes na conjuntura do crime cibernético atual. São elas a vítima solitária, a vítima ignorante, a vítima idosa, a vítima criança ou adolescente, a vítima gananciosa e a vítima curiosa.

A vítima solitária nos traz o entendimento de que a informática preza pela individualidade, de um lado aproxima as pessoas, permitindo maior velocidade e intensidade nos contatos, através de e-mails, redes sociais, mensagens; mas por outro lado restringe o contato físico entre humanos diminuindo a sociabilidade. Duas são as formas de solidão que podem ser consideradas para este trabalho. Uma delas é a solidão antissocial, onde existe a falta de convívio real no meio social, estas vítimas são mais propensas a procurar refúgio no meio virtual, utilizando-se muitas vezes de sites pornográficos, sendo grande a proporção de golpes que se camuflam nestes meios para se instalarem. Assim, os usuários mais sociáveis possuem menor exposição a riscos do que os usuários antissociais, pois estes têm a tendência a aceitar materiais de conteúdo sexual reduzida. Os usuários antissociais desenvolvem um risco maior, pois para suprir carências pessoais, buscam na rede satisfações, sendo alvos fáceis dos convites à visualização de materiais pornográficos que escondem códigos maliciosos. Diante disso, é de se notar que a solidão física prolongada juntamente com o acesso a sites pornográficos seria capaz de aumentar o potencial de vitimização do usuário[88].

---

[86] LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2. ed. São Paulo: Atlas, 2011. p. 36.
[87] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 183.
[88] Ibidem, pp. 188-190.

Outra forma é a solidão relacional, onde o usuário por falta de companhia, e não por possuir características antissociais, pois estes diferentes daqueles, possuem o desejo de se sociabilizar, acabam por sucumbir a ambientes virtuais em busca de pessoas com afinidades, grupos semelhantes e relacionamentos afetivos. Um dos principais usos da rede são os relacionamentos sociais como por exemplos e-mail, aplicativos de relacionamentos e redes sociais. Porém, muitas vezes esses métodos são utilizados como armadilhas com o objetivo de conseguir informações privilegiadas das vítimas, ou seja, a solidão relacional faz com que o usuário se interesse em novas companhias e costumam confiar em serviços que auxiliam e apoiam para tais fins, tendo, por conta da emoção advinda do estado de isolamento, certas capacidades cognitivas diminuídas. Desta forma o criminoso virtual, ao conhecer essas particularidades, explora tal estado emocional.

Outro tipo de vítima é a ignorante, nesta etapa é preciso se analisar a compreensão do usuário informático, o que imediatamente pressupõe algum conhecimento em informática. A ignorância referida deverá ser vista do aspecto dos riscos da rede onde há o desconhecimento quanto à periculosidade da rede mundial de computadores, porém o argumento de desconhecimento dos riscos é de difícil aceitação, tendo em vista a larga divulgação da mídia. Outra hipótese de ignorância é a tecnológica. Como apenas a menor parte dos usuários possuem sólidos conhecimentos técnicos, a falta de tais noções é a porta de entrada para individuo mal-intencionados aplicarem golpes. A parcela de culpa por parte do individuo ignorante, depende do grau de evitabilidade ou de imprudência[89].

Um tipo especial de vítima é a idosa, pois esta, protegida pelo Estatuto do Idoso, Lei nº 10.741/2003, possui tratamento diferenciado em varias esferas. Os crimes cometidos contra cidadão com idade acima de sessenta anos, enquadram-se em uma categoria onde o seu cometimento será tido como uma agravante da pena, por levar-se em conta a natural fragilidade dessa classe de indivíduos. Reforço quanto ao argumento de especial importância está no art.61, II, h do Código Penal, que foi alterado pela Lei nº 10.741, acrescendo-se que a vítima por ser idosa é um agravante da pena[90].

Normalmente a rotina das pessoas de idade, quando usuárias da rede, frequentam ambientes de bastante interesse dos criminosos, como por exemplo, salas de bate-papos, além disso, o envelhecimento traz consigo, outras características que influenciam diretamente a vitimização: são algumas delas a dificuldade acentuada em adaptar-se a novas tecnologias e sua linguagem, a não compreensão de certos serviços ofertados pela informática e, principalmen-

[89] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. pp. 193-196.
[90] Ibidem, pp. 196-198.

te, a não compreensão dos valores dos bens jurídicos virtuais, o desconhecimento de limites das atitudes dos delinquentes e o potencial prejuízo da ação delituosa[91].

Estes desconhecimentos acabam ocasionando uma fragilidade especial no que toca à imprudência de navegação, como por exemplo, a imprudência na instalação de programas, na atualização de sistemas de proteção, e até mesmo na crença exagerada de noticias enganosas ou falsa identidade.

Outro tipo de vítima que recebe proteção especial do ordenamento jurídico é a criança e o adolescente. Os diferentes estágios da vida exigem cuidados diferenciados quanto à educação e restrição de exposição aos riscos, ou seja, crianças e adolescentes são vítimas diferentes, expostas a riscos diversos na rede mundial de computadores, especialmente no que tange a suscetibilidade quanto à criminalidade, vista que ambas as condutas são graves, porém a vitimização da criança relata atitude de maior reprovabilidade, pois é de se compreender que a infância é uma faixa de idade de alta suscetibilidade, de influências passivas em que a construção do caráter se dar de modo mais intenso.

Ao se atingir certa etapa de amadurecimento os indivíduos adolescentes passam a ser usuários mais capazes de se proteger, tornando-se assim alvos mais difíceis do que as crianças, por sua vez, as crianças, em regra necessitam de navegação supervisionada, pois estas são mais tendentes a serem influenciadas pelo conteúdo acessado. A criança mostra-se um alvo fácil especialmente por acreditar em fantasias, historias e promessas, não tendo maturidades suficientes para perceber riscos com antecedências.

Utilizando da fragilidade advinda da idade, os criminosos utilizam-se de salas de bate-papo com temas infantis, fazendo-se passar por crianças com o objetivo de aliciarem interesse sexual, muitas vezes oferecendo presentes para conquistar a confiança das vítimas. Visto isso mostra-se que a internet é um ambiente de grande potencial para influenciar negativamente, levando as crianças e adolescentes, muitas vezes a absorverem e acostumarem-se com material inadequado para sua faixa de idade. Há, todavia, material de boa estirpe, que auxilia no desenvolvimento intelectual, levando ao incentivo do aprendizado, voltado para a faixa etária de crianças e adolescentes. Sendo assim, é de se concluir que mesmo havendo uma maior fragilidade quanto à criança, os riscos provenientes do ambiente virtual, também englobam os indivíduos adolescentes, que não deixam de ser um dos alvos preferenciais dos criminosos[92].

A vítima gananciosa, por sua vez é aquela que busca ativamente modificar a sua situação de fato, atentando ascensão social ou econômica, ou outra vantagem estritamente pesso-

[91] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 198.
[92] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. pp. 198-202.

al. Trata-se de um sentimento negativo e egoísta de alguém que busca ter para si grande quantidade de poder. Com isso individuo que nota a possibilidade patrimonial tem as suas atitudes transformadas agindo com menor cautela, assumindo maiores riscos e chegando até a prejudicar terceiros para atingir seus objetivos, esses indivíduos enquadram-se especialmente no rol das vítimas de crimes patrimoniais e de estelionatos, pois sua capacidade de raciocínio ponderativo se encontra parcialmente encoberta por ideias hedonistas ou de avareza. Somando-se a isso a falta de cautelas quanto aos riscos do mundo virtual, ocasionando assim, grandes quantidades de estelionatos, por exemplo,[93].

É exemplo da forma de ação dos criminosos no meio virtual que induzem a vítima gananciosa: raspadinhas virtuais, falsos sorteios de prêmios ou participação em programas de televisão, mensagem na tela informando que o usuário foi o milionésimo a acessar o site e ganhará um prêmio, promessas de empregos com altos salários, essas são apenas algumas estratégias que visam explorar a ganância dos usuários, no intuito de persuadi-los, ceder informações, ou entrar em site. Assim vemos que o estado de ganância tem servido como facilitador para execução dos informáticos que se utilizam do argumento do prêmio, do brinde ou do grátis pra auferir lucros[94].

Para finalizar, falaremos agora sobre a vítima curiosa. Trata-se de um tipo de vítima que diferentemente da vítima ignorante, que sofre com ações que exploram a sua vulnerabilidade técnica ou sua incapacidade de compreender os riscos da tecnologia, a vítima curiosa pode não ter vulnerabilidade alguma em tais áreas.

A rede mundial de computadores mostra-se como um portal de infinitas informações, umas de extrema qualidade outras nem tanto, porém ambas são território da curiosidade dos internautas, essa curiosidade pode ser exercida de forma responsável como também podem ser exercida com irresponsabilidade e a exploração do ambiente virtual, quando feita com imprudência, poderão ser perigosos. Spencer Toth Sydow, neste sentido:

> Exceto em países como a China (que proíbe pornografia de qualquer gênero) e o Japão (que penaliza a exibição dos órgãos genitais), além das restrições havidas nas legislações árabes e muçulmanas, grande parte da civilização tem acesso amplo a multimídia sobre sexualidade, cabendo ao adulto buscar as informações que mais lhe pertinem ou interessam[95].

Exceto a china e em alguns outros países, a rede mundial é aberta, permitindo liberdade de circulação e acesso as informações, com isso vários usuários aproveitam essa facilidade

[93] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. pp. 202-205.
[94] Ibidem, pp. 202-205.
[95] Ibidem, p. 207.

e apresentam curiosidade mórbida, abstrata, de índole sexual ou de lucro, com isso as aplicações de golpes virtuais se efetivam e através de armadilhas atrai os usuários. Assim, surge o questionamento de até que ponto pode uma curiosidade influenciar nas condutas preventivas dos usuários pondo em risco a sua segurança[96].

Evidente que ao utilizar-se da rede mundial de internet os usuários não estão 100% seguros, pois como citado anteriormente existe uma vasta gama de golpes, dentre os mais populares estão o golpe do boleto, onde a vítima é ludibriada e acaba efetuando um pagamento a um estelionatário, falsos e-mails de instituições financeiras, anúncios de oportunidades de emprego falsas, furto de identidade com o objetivo de obter vantagens ilícitas, como por exemplo, abrir uma empresa fantasma em nome de outra pessoa, romances pela internet, que tem se mostrado por demais perigosos, pois na verdade nunca se sabe quem é a pessoa com a qual está se comunicando, entre outros que vem acometendo a população. Porém, está claro que a principal arma a favor das pessoas é a prudência, pois as falhas do sistema existem, não há o quê questionar e o fator humano, comprovadamente, tem sido a principal porta de entrada para a instauração dos golpes, sendo assim a precaução o que resta.

[96] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. pp. 206-208.

CAPÍTULO 3 – SEGURANÇA, COMBATE E ASPÉCTOS JURÍDICOS.

3.1 Formas de Proteção

Como visto anteriormente, na internet nada é 100% seguro, sendo assim, qualquer pessoa pode ser vítima. Todos os dias ofensas são proferidas nas redes sociais, pessoas recebem cobranças indevidas, contas são saqueadas, por isso, é importante que os usurários da rede estejam cientes dos riscos contidos nos hábitos cotidianos que por eles são executados, prevenindo-se de um eventual problema. Pensando nisso, alguns órgãos governamentais brasileiros se dedicam a desenvolver um conjunto de ações visando o uso ético, responsável e seguro da internet no Brasil, tendo por objetivo estimular os usuários ao uso da internet com segurança[97]. É notório que essa falta de segurança existente no ambiente virtual muitas vezes não é sentida pelos usuários, que se utilizam dos serviços oferecidos pela internet, e não imaginam que podem ser vítimas de um delito.

As cartilhas, que demonstram as formas de utilizações da internet com mais segurança, são exemplos das ações desenvolvidas por esses órgãos governamentais, estando estas disponíveis em formato PDF ou na forma ilustrada, geralmente não havendo restrições na sua divulgação. No site do Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) o leitor poderá ter acesso a vários fascículos para download, bastando para isso acessar o link: http://cartilha.cert.br/. O material produzido tem a finalidade de ajudar os usuários da internet a usufruir da rede com mais segurança[98]. Mas, além de informações sobre segurança na internet, os usuários também precisam colocar em prática o conteúdo destas informações, pois um estudo feito pela companhia de segurança digital McAfee em 2012, indicou que 15,5% dos computadores do Brasil não possuem software contra ameaças virtuais instalados[99], tornando-os vulneráveis a ataques de invasores, ou seja, de um lado nos deparamos com a falta de informação e do outro lado com o descaso dos usuários quanto aos cuidados ao se utilizar do espaço virtual, a soma destes e outros motivos, tais como a falta de recursos tecnológicos no que diz respeito às defesas técnicas do sistema tornam o ambiente virtual um local inseguro e propenso a delitos.

---

[97] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 41.
[98] Ibidem, p. 41.
[99] **NO BRASIL 16 DOS PCS TEM PROTEÇÃO ZERO CONTRA AMEAÇAS, DIZ ESTUDOS**. Disponível em: <http://www.crimespelainternet.com.br/no-brasil-16-dos-pcs-tem-protecao-zero-contra-ameacas-diz-estudo/>. Acesso em: 19/10/15.

Evidentemente que um bom antivírus é um software obrigatório a qualquer computador, no entanto as atualizações que devem ser feitas periodicamente influenciarão caso não sejam observadas. Do mais, o sistema operacional e os programas, quando atualizados, também ajudam na proteção do sistema. Estes devem ser originais para que possa haver as devidas atualizações. Quanto ao antivírus, é um software obrigatório em qualquer computador. Segundo Cassanti.

> Um bom antivírus é capaz de identificar e eliminar phishing, spyware, rootkit e deveter ainda sistemas para verificar vírus em e-mail, mensageiros e programas de trocas de arquivos p2p. Esses programas estão sempre à procura de novas ameaças que se disseminam na web, por isso existem atualizações diárias que mantêm a segurança[100].

Ao adquirir um antivírus é recomendável que este seja de um fabricante conhecido, pois existem antivírus falsos que fazem uma suposta varredura nos arquivos, são os chamados scareware. Tratam-se de golpes que tentam ludibriar os usuários a comprar um antivírus falso, sendo assim, mesmo que não seja possível a aquisição de uma proteção paga, a opção por um software gratuito, ainda assim será válida, contanto que seja de uma empresa conhecida, porém nunca devemos deixar o sistema operacional completamente desprotegido. Outro ponto importante a respeito das formas de proteção é o que diz respeito à instalação de dois antivírus, pois esta ação prejudicará o desempenho da máquina e acabará havendo uma incompatibilidade, ou seja, um atrapalhará a ação do outro[101].

Ter um computador bem configurado diminui a possibilidade de ataques, pois os invasores procuram um ambiente vulnerável, os usuários são os principais responsáveis por incidentes, e a sua forma de navegação determinará o grau de perigo ao qual o mesmo irá se expor. Dentre os cuidados mais conhecidos com a proteção, podemos citar os seguintes: nunca clicar em links que o direcione para sites desconhecidos sem antes verificar o seu destino, essa verificação poderá ser feita com um clique sobre o link com o botão direito do mouse e escolher a opção verificar propriedades. Um simples gesto como este pode vir a evitar futuros problemas.

Ao se cadastrar em sites é importante que se verifique a procedência do mesmo, com isso pode ser evitado que se caia em um golpe, pois muitos sites têm registros de atividades ilegais e mesmo assim permanecem em pleno funcionamento fazendo mais vítimas, uma atenção especial deve ser dada quando determinado site pede informações referentes ao número de cartões de crédito, pois este poderá ser clonado ou as suas informações poderão ser

[100] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 43.
[101] Ibidem, p. 43.

repassadas para empresas que se utilizarão destas posteriormente. Mais adiante falaremos melhor a este respeito.

O simples fato de utilizar navegadores diferentes para operações distintas poderá ser algo que venha a evitar um problema, por exemplo, se usar um navegador para determinados sites, como por exemplo, blogs, notícias, fóruns, e outro para sites de banco, por exemplo, caso o navegador costumeiramente utilizado para acessar blogs venha a serem infectados por vírus, estes vírus não poderão afetar as operações feitas através do outro navegador.

Quanto aos serviços que exigem um nome para o usuário e uma senha para que se possa entrar no site, estes devem ser prestados com cautela, pois muitas vezes os usuários saem do serviço apenas clicando no botão vermelho, localizado na parte superior da página, e este ato faz com que o site continue aberto, deixando-o disponível para qualquer pessoa que venha posteriormente utilizar a máquina, ter acesso às informações do usuário. Diversos são os crimes que podem vir a ser consumados por causa de falhas deste tipo, dentre eles, podemos citar os crimes contra a honra, o furto de senha, furto de perfil, acesso a número de conta bancaria, furto de identidade, entre outros.

A dificuldade das senhas é outro fator que deve ser levado em consideração, criar senhas difíceis e mudá-las periodicamente diminuirá as chances da ocorrência de um crime virtual. As senhas são intransferíveis, particulares e sigilosas, elas são os principais meio de proteção contra o acesso indesejado de terceiros ao seu computador. Muitas vezes os usuários se utilizam de senhas demasiadamente fracas, como por exemplo, sua data de nascimento, o nome de algum parente ou uma sequência óbvia de números.

Para que o seu sistema tenha uma melhor segurança é necessário que as senhas utilizadas sejam fortes, como por exemplo, a combinação de letras e números, a criação de senhas longas, a inserção de pontos, vírgulas, arrobas e números como também a misturas de letra maiúsculas e minúsculas, e é muito importante que se tenha uma senha diferente para cada serviço.

Como podemos ver, os usuários do mundo virtual são grandes colaboradores para sua situação de vítima, um assunto importante é o que diz respeito às compras feitas pela internet. Muitas são as vantagens em fazer compras no ambiente virtual, como por exemplo, não ter que sair de casa, por este e outros motivos o mercado de compras virtuais só vem crescendo no país e no mundo. No entanto, este mercado além de atrair novos consumidores, também atrai golpistas[102].

[102] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 46.

Um dos riscos que o usuário consumidor de mercadorias adquiridas através do meio virtual, é de não receber produto nenhum ou este vir com avaria, trocado ou com qualidade bem abaixo do anunciado, configurando-se uma propaganda enganosa, por isso desconfie de mercadorias muito abaixo do preço de mercado, antes de efetuar a compra deve ser verificado a índole do site onde pretende comprar, e se o mesmo possui reclamações. Outro risco sofrido pelo o usuário é a respeito dos seus dados pessoais, pois este pode vir a ser utilizados por estelionatários. Para se prevenirem destes problemas as compras devem ser negociadas com site seguros e conhecidos, pois qualquer um pode anunciar produtos na internet. Imprimir e guardar registro de suas transações online pode vir a ser útil posteriormente, pois esta será a principal forma de comprovar que houve um contrato de compra e venda via internet. Caso venha a ocorrer algum tipo de problema no que diz respeito à compra deverá ser registrado uma reclamação no PROCON de sua cidade sobre a loja virtual, a respeito disto trataremos melhor no próximo tópico.

Existe a possibilidade de criminosos clonarem a página de um site, levando os usuários a acreditar que estão em uma loja de confiança, por isso é preciso haver a prudência quanto ao recebimento de e-mails com promoções que indiquem um link, mesmo quando estes aparentemente são de uma loja onde o usuário já é cadastrado. As vantagens que são oferecidas nas comprar via internet, também são existentes nas transações bancárias, devendo neste caso ter mais precaução, pois mesmo o setor bancário ser o que mais investe em tecnologia, este também é um dos mais visados pelos criminosos.

O e-mail é um dos meios mais utilizados pelos atacantes, valendo-se de termos de notificações e nomes de instituições financeiras para atrair as vítimas, estes agentes utilizam-se do medo dos usuários enviando-lhes e-mails, como por exemplo, notificando a respeito de um suposto cheque protestado ou uma intimação, palavras como ‘‘fatura’’, ‘‘pagamento’’ e ‘‘alerta’’, e-mails com mensagens que despertam a curiosidade, com palavras do tipo: fotos em anexo, vídeo íntimo de artista famoso e fotos de traição, juntamente com mensagens que despertam a ganância, são os títulos mais utilizados para a aplicação desse golpe. Em todos esses exemplos apresentados, a participação do usuário para a propagação do golpe é fundamental, pois os atacantes procuram induzi-los a executar alguma tarefa, no entanto, sem esse auxílio o ataque não terá sucesso[103].

As salas de bate papo; uma das opções de uso mais populares na internet, estas tem como principal característica preservar o anonimato ao mesmo tempo em que proporciona en-

[103] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 50.

tretenimento, porém esse anonimato muitas vezes pode estar camuflando uma situação de perigo onde o usuário se deixa levar pelo divertimento e caba por cair nas mãos de um golpista, pois não se sabe realmente quem está do outro lado. Nas salas de bate papo, o golpista envolve as suas futuras vítimas, ganhando a sua confiança, e aos poucos são convencidas a fornecer os seus dados pessoais, tais com endereço residencial, telefone, etc. Os golpistas têm preferência por crianças e adolescentes, pois estes, em regra, são mais audaciosos ao utilizar o ambiente virtual e muitas vezes não tomam os devidos cuidados, as crianças, particularmente, por sua pouca idade e inexperiência tecnológica, podem vir a sucumbir a armadilhas de agentes mal intencionados sendo presas fáceis para ataques de pedofilia, já os adolescentes, são usuários mais ousados e procuram desvendar os "segredos" do sistema, muitas vezes não se importando com os riscos, porém ambos estão expostos a ataques de toda espécie, pois nenhum tipo de delito que possa afetar as crianças, também não possa ser empregado aos adolescentes, apenas o que os diferencia é o tipo de navegação. Quanto aos adultos, estes também costumam cair nos golpes aplicados através das salas de bate papo. Ações simples como não divulgar informações confidenciais, fotografias, vídeos pessoais, evitar marcar encontros com desconhecidos, pois é fácil mentir e fingir ser outra pessoa na internet, tendo em vista que tempo de conversa não garante a veracidade das informações[104].

Ao se tratar de segurança, todo o cuidado nunca é demais, por esse motivo que o assunto prevenção, no que concerne o ambiente virtual deve vir como fator primordial a ser utilizado pelos usuários e como o nosso objeto de pesquisa tem por escopo levar ao conhecimento da população entendimento acerca dos delitos virtuais e com a utilização destes seja possível contribuir de alguma forma para a atenuação dos crimes cibernéticos, nada mais justo do que se falar em prevenção, suas formas, e mostrar o quanto essa é fundamental para que melhor sejam utilizados os serviços que a rede mundial de internet tem a oferecer.

3.2 Como Agir em Caso de Crimes Virtuais

Muitas vezes quando nos deparamos com uma situação que feri nossos direitos como cidadão, e como pessoas não sabem como agir, nos crimes virtuais não são diferentes. Na maioria das vezes a vítima de um crime cibernético, apesar de toda a indignação, desconforto e prejuízo que sofreu não procurar os seus direitos e sucumbe a uma situação de esquecimento, aumentando assim o rol dos crimes que não foram quantificados, ou seja, trata-se de con-

[104] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 41.

dutas delitivas praticadas por agentes no ambiente virtual que nunca chegaram ao conhecimento da justiça, pois as vítimas não procuraram a justiça, talvez por falta de conhecimento, medo ou por achar que para aquele problema não há punição.

A punição do criminoso poderá ocorrer da mesma forma como a punição de qualquer outro tipo de crime, porém para se chegar ao autor do crime cibernético, é importante que seja tomada algumas providências, como por exemplo, a preservação das evidências do crime, o simples ato de imprimir e salvar os arquivos, e-mails, telas, páginas da internet, ou seja, tudo o que possa comprovar o crime, definirá a possibilidade de punição ou não. Tendo em vista que as evidências no mundo virtual podem desaparecer por completo, não deixando rastro algum para que seja encontrado o criminoso e que todas as provas são de suma importância para a investigação da polícia, estas devem ser registradas em cartório em ata notarial, sendo assim adquirirão validade jurídica e terão a possibilidade de ser posteriormente utilizadas na justiça[105].

A ata notarial é um documento instrumento público por meio do qual o tabelião ou preposto, a pedido da pessoa interessada, vai constatar todo o ocorrido com fidelidade dos fatos, portando por fé que tudo aquilo relatado pela vítima representa a verdade plena. Este ato será redigido e lavrado por um tabelião de notas em livro próprio. Esta poderá ser utilizada para comprovar fatos ocorridos na internet, como por exemplo, certificando o conteúdo divulgado em páginas da internet, textos que contenham calúnia, injúria e/ou difamação, uso indevido de imagens, infrações a direitos autorais, entre outras atitudes que possam atingir o bem jurídico de terceiros. A ata notarial servirá para pré-constituir prova dos fatos, pois muitas vezes a prova de determinadas situações é por demais dificultosas, neste caso o tabelião servirá como testemunha oficial cujo ato vai desencadear a fé pública, podendo ser utilizado no tribunal, pois os livros e arquivos dos tabeliões não têm prazo de validade, sendo mantidos sempre em local seguro e apropriado [106]. Estas atas podem ser requeridas diretamente a um tabelião, sendo dispensável a presença de um advogado.

Outro documento de grande importância é o boletim de ocorrência, no caso de crimes cibernéticos, é feito em qualquer delegacia de polícia, não sendo necessário ir a uma delegacia especializada em crimes virtuais, tendo em vista que muitas cidades não as possuem. Para registrar a ocorrência de um crime cometido por intermédio da internet, a vítima deverá de posse das provas, como citado em tópico anterior, procurar a delegacia mais próxima.

---

[105] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. pp. 56-57.
[106] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 57.

Em Pernambuco a polícia civil disponibiliza do serviço da Delegacia Pela Internet onde as vítimas de crimes, tanto cibernéticos, quanto cometidos de forma convencional, terão a facilidade de registrar um boletim de ocorrência sem precisar sair de casa, dentre os serviços prestados estão a denúncia de roubos e furtos[107] . O boletim eletrônico possui o mesmo valor de uma ocorrência registrada em uma delegacia física, pois se trata de um documento oficial emitido pela Polícia Civil do Estado de Pernambuco. O procedimento é simples e seguro, bastando apenas a vítima registrar as informações on-line, em seguida um policial entrará em contato com a mesma para confirmar alguns dados e em seguida efetivar o registro do boletim de ocorrência. Essas informações serão encaminhadas para as delegacias da área onde o fato ocorreu. A vítima terá um prazo de seis meses, após o registro do boletim eletrônico, para fazer a representação da ocorrência, pois, por tratar-se de crimes de natureza privada, será necessário que a pessoa atingida solicite, de forma presencial, a continuidade das investigações[108].

É essencial que as vítimas saibam a forma correta de como agir ao procurar os seus direitos, pois sabemos que muitas destas pessoas não possuem sequer um conhecimento básico sobre tecnologia informática, tendo isso em vista, o objetivo desta pesquisa é levar ao cidadão comum algum esclarecimento acerca de como deverá proceder caso venha a ser vítima de um crime dessa natureza. Assim, explanaremos a seguir algumas formas básicas de procedimento que poderão orientar neste sentido.

Inicialmente falaremos dos casos de ameaça executados através de e-mails, em casos como estes a vítima deverá agir de forma que possa facilitar a persecução do agente, preservando o conteúdo das mensagens, e o cabeçalho do e-mail, ou seja, onde se encontra localizado o nome e endereço do remetente, assim como também data e hora da transmissão. Em seguida esse material deverá ser impresso como prova e levado a uma delegacia mais próxima. Caso a vitima precise ter acesso a mais informação, que só possam ser fornecidas pelo provedor, esta poderá ser obtida através de uma ordem judicial, onde será requerido que o mesmo informe a quem pertence o IP (protocolo de internet) solicitado[109]. Através do IP será possível que seja localizado o usuário que cometeu o ato ilícito.

Para que haja o crime contra a honra precisará existir publicidade destas mensagens, ou seja, se um e-mail desonroso for enviado único e exclusivamente à pessoa alvo dos insultos, isto, por si só, não se configurará como um crime contra a honra por faltar o requisito pu-

[107] **DELEGACIA PELA INTERNET**. Disponível em: <http://servicos.sds.pe.gov.br/delegacia/> Acesso em: 22/10/2015.
[108] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 59.
[109] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 66.

blicidade, porém a partir do momento que estas mensagens desonrosas forem enviadas para terceiros, maculando a imagem da vítima, isso sim configurar-se-á um crime contra a honra perpetrado de forma virtual[110].

O site SaferNet, é uma organização não governamental em parceria com o Ministério público Federal que reúne especialistas para combater crimes digitais, em sua página o usuário poderá denunciar, de forma anônima, qualquer crime ou violação aos direitos humanos praticados através da internet. Em oito anos a SaferNet Brasil recebeu e processou 3.606.419 denúncias anônimas envolvendo 585.778 páginas distintas escritas em nove idiomas e hospedadas em 72.739 hosts diferentes, conectados à internet através de 41.354 números IPs distintos, atribuídos para 96 países em cinco continentes[111]. Outro site brasileiro que está a serviço da população é o Digi Denúncias, através dele a vítima poderá efetuar as denúncias de crime eletrônico optando em manter o anonimato ou não, a ocorrência poderá ser registrada a partir de qualquer lugar do país e em seguida será analisada pelo Ministério Público Federal[112].

Outro golpe muito praticado é o de estelionato, o procedimento que deverá ser tomado pelas vítimas será semelhante ao de ameaça, citado anteriormente, ou seja, imprimir e preservar todas as provas e de posse destas, procurar a delegacia mais próxima para registrar a ocorrência. Quando o estelionato envolve cartões de crédito, o titular do cartão deverá imediatamente entrar em contato com a empresa prestadora do serviço com o objetivo de cancelar o crédito, mas na maioria das vezes os usuários só percebem que foram vítimas de golpes envolvendo o seu cartão quando a fraude já está instaurada, mesmo assim as providências citadas acima devem ser tomadas e a vítima deverá procurar a justiça.

Como já mencionado, os golpes de estelionato no Brasil são os mais executados. O procedimento tomado por quem foi vítima desses crimes será semelhante aos dos crimes contra a honra, ou seja, imprimir e preservar todas as provas e procurar a delegacia mais próxima para registrar a ocorrência, mesmo a vítima não tendo acesso a uma delegacia especializada[113]. Quanto às fraudes envolvendo cartões de crédito, grande parte delas dizem respeito a falsificações. Ao se adquirir um produto utilizando-se do cartão de crédito, dados pessoais do usuário ficam armazenados na empresa que efetuou a venda, sendo assim, caso a empresa venha a sofrer alguma invasão a seu sistema, os agentes poderão ter acesso aos dados dos clientes e vir a utilizá-los.

---

[110] Idem, p. 66.
[111] **SAFERNET BRASIL.** Disponível em: http://new.safernet.org.br/. Acesso em: 23/10/2015.
[112] **DIGI DENÚNCIA**. Disponível em: http://www.prsp.mpf.gov.br/noticias-prsp/aplicativos/digi-denuncia. Acesso em: 23/10/2015.
[113] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 73.

Muitos casos não poderão ser resolvidos pela própria administradora do cartão, nestes casos um boletim de ocorrência deve ser feito e todo o processo deve ser documentado, guardando cópias do relatório policial para apresentar a instituição financeira se for preciso, provando assim a fraude. Caso a instituição financeira não estorne as cobranças indevidas o cliente deverá formalizar reclamações em um Órgão de Defesa do Consumidor, no juizado especial cível ou na justiça comum[114].

Juntamente com as fraudes envolvendo cartões de crédito estão problemas relacionados às compras feitas pela internet, estas podem ser efetuadas por qualquer pessoa, em qualquer parte do planeta, desde que haja conexão com internet. Os usuários da rede podem adquirir produtos de lojas virtuais utilizando-se de transferência bancário, cartões de crédito ou boletos bancário. Ao utilizar este método de compra se faz necessário que o consumidor tenha alguns cuidados, tais como, verificar a autenticidade do site que oferece o produto, registrar todas as etapas da compra, pois estas em uma ação futura servirão como meio de prova, e se assegurar quanto à segurança do aparelho que será utilizado para se fazer à operação, pois este método além de ser recente, também comporta seus riscos.

Antes de efetuar uma compra via internet, o consumidor deve, sempre que possível, procurar informações sobre o site, no que diz respeito à reputação das lojas e serviços, devendo sempre dar preferência a sítios que informe o seu endereço físico e outras informações necessárias para que o consumidor possa o localizar. O consumidor também tem a seu favor sites que mostram a reputação das empresas, como por exemplo, o Reclame Aqui[115], através deste é possível averiguar a qualificação de determinada loja física e/ou virtual, como também efetuar reclamações ou atribuir qualidades positivas às mesmas e o PROCON (programa de proteção e defesa do consumidor), onde poderão ser registradas reclamações. O consumidor virtual deve ficar atento, pois muitas vezes trata-se de golpes aplicados por empresas que sequer existem e vendem produtos no ambiente virtual como forma de armadilhas para enganar os consumidores, em caso de dúvida, a vítima deve recorrer diretamente à delegacia mais próxima, lá serão prestados os esclarecimentos de como proceder.

Mais um problema da era cibernética é o furto de perfis. O termo perfil é utilizado para designar a imagem do uma pessoa no ambiente virtual, esta representação pode ou não possuir as mesmas características do proprietário, porém o representa no ambiente virtual. Os mesmos podem ter diversas finalidades, tais como: profissionais, comerciais ou artísticas. Mesmo tratando-se de algo intangível, ou seja, bens incorpóreos, o proprietário do perfil pos-

[114] CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014. p. 75.
[115] **RECLAME AQUI**. Disponível em: http://www.reclameaqui.com.br/. Acesso em: 23/10/2015.

sui diretos sobre estes. Por isso devem ser preservados. O agente que, ao se apoderar de perfil alheio, e através deste procurar auferir vantagens ou agir de forma indevida, poderá se enquadrar no crime previsto no art. 307 do Código Penal, ou seja, falsidade ideológica, com pena de detenção de 3 meses a 1 ano ou multa, isso se o fato não constituir elemento de crime mais grave. A denúncia poderá ser prestada ao próprio provedor de serviço onde está hospedado o perfil. Sites como o Facebook, Twitter, YouTube , possuem ferramentas destinada a denunciar esse tipo de fraude.

É essencial que as vítimas saibam a forma correta de agir ao se depararem com esses crimes, por exemplo, ao ter consciência do quanto à preservação das provas é importante, pois sabemos que as explicações que aqui foram dadas, certamente servirão como base para o combate dos demais crimes cibernéticos que não foram citados neste trabalho, mesmo que esse trabalho sirva de orientação, é de suma importância que as vítimas procurem as autoridades, pois somente estas poderão tomar as devidas providências.

3.3 Análises do Marco Civil e da Lei nº 12.734/12

Sobre o que tange o Direito Informático Brasileiro, muito se tem falado sobre o tema, porém, de nada adianta a criação de projetos ou normas se não for verificado a existência de estrutura e aplicabilidade de tais regras, pois para serem tratados os delitos informáticos se faz necessário pessoal especializado e equipamento de última geração, sem falar que em muitos dos crimes informáticos, para haver sua persecução é preciso conexão de alta qualidade e apoio de países de todo o mundo para que as investigações não esbarem em formalidades e entraves burocráticos.[116] E infelizmente o que vemos na realidade do país são profissionais despreparados e equipamentos defasados, assim impossibilitando até as investigações. É sabido que os agentes de alguns desses crimes contam com equipamentos de última geração e são dotados de uma capacidade técnica considerável, como exemplos podem citar os invasores de sistema bancário. São delitos de difícil contenção, previsão e visualização, tendo em vista que o delinquente, normalmente preocupa-se em não deixar vestígios.

Nesse sentido o marco civil da internet brasileira, aprovado em 23 de abril de 2014, entrando em vigor no dia 23 de junho de 2014, tendo como objetivo regulamentar questões relativas ao Direito Informático regrará as circunstâncias de atuação dos provedores e dos usuários, limitando eventuais abusos do poder público. Conforme exposto no seu art. 1°, ao deixar

[116] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 200.

claro que a lei estabelecerá os princípios, garantias, direitos e deveres para o uso da internet no Brasil e ainda definindo as diretrizes de atuação da União, Estados, Distrito Federal e Municípios quanto à matéria.

A necessidade de uma lei que regulasse direitos e deveres dos usuários e provedores quanto ao uso da internet no país, em meados do ano de 2009 voltou à tona essa discussão, porém só no ano de 2013, impulsionado pelas denúncias do então funcionário do governo americano, o administrador de sistemas, Edward Snowden, que na época revelou uma série de documentos contendo informações sigilosas da NSA (National Security Agency), este tornou mundialmente conhecidos os métodos de espionagem do governo americano, mostrando com isso que, a tecnologia ocidental era na verdade uma "máquina de vigilância". O informante trouxe a tona informações que diziam respeito até mesmo ao Brasil, quando divulgou que a NSA conseguiu espionar a rede virtual privada da Petrobras (conforme divulgado pelo programa semanal Fantástico da tv Globo). Motivado por esse escândalo, que deixou abalado a soberania nacional, foi acelerado a aprovação do Marco Civil da Internet, passando assim a ser regulamentada a privacidade on-line do povo brasileiro[117]. Nota-se que foi preciso a existência de um escândalo envolvendo a soberania nacional para que houvesse a aprovação de uma lei que há tempos a sociedade brasileira necessitava.

Mesmo tratando-se de uma lei eminentemente civil, nos utilizaremos do Marco Civil da internet por este ter papel fundamental no que tange o estudo da criminalidade informática, pois esta lei pode ser considerada como uma norma inauguradora do direito virtual, buscando a criação de margens seguras para deveres e responsabilidades aos usuários e aos prestadores de serviços na internet. Nos parágrafos a seguir, analisaremos alguns artigos que são de considerável importância para o nosso trabalho.

Conclui-se que o art. 4°em seu inciso I, do Marco civil da internet, ao falar que "o acesso à internet é direito de todos", está passando o entendimento de um direito difuso e universal. Já no seu art. 5°, ao utilizar-se da denominação "terminal", esclarece que os crimes cibernéticos não são apenas praticados por computadores, mas sim por qualquer dispositivo eletrônico que seja capaz de manipular dados, ou seja, que possa executar condutas praticadas no mundo virtual[118].

A realidade atual traz a necessidade de haver uma proteção no que diz respeito a certos valores como, por exemplo, inviolabilidade das comunicações e dados dos usuários. No que

[117] MENNA, Ricardo de Macedo B. **Direito e Redes Sociais na Internet: A Proteção do Consumidor no Comércio Eletrônico.** 2. ed. Curitiba: Juruá, 2014. p. 104.
[118] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p 275.

diz respeito aos dados informáticos, o Marco Civil regulamenta-os no seu artigo 22, deixando evidente que o acesso por parte de terceiros aos dados dos titulares, apenas será possível por intermédio de autorização judicial. O particular interessado poderá requerer ao juiz competente as informações com a finalidade de compor conjunto probatório, porém este requerimento deve demonstrar explicitamente os indícios da ocorrência do delito, a justificativa motivada da utilidade dos registros e o período ao qual se referem. Do exposto no art. 11 da Lei nº 12.965/14 quanto à competência para a obtenção das informações, será levado em conta o princípio da territorialidade.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

A respeito do provedor da internet, este terá a sua responsabilidade regulamentada nos arts. 18 e 19 do dispositivo supracitado, os mesmos não se responsabilizando por danos decorrentes de conteúdo gerado por terceiros, no entanto surgirá responsabilidade caso estes venham a receber ordem judicial e não tornar indisponível conteúdo apontado como infringente. Porém a legislação existente até o momento, não regra eventuais responsabilidades penais, sendo assim o provedor terá a prerrogativa de dispensar formalismos processuais em situações que envolvam imagens, vídeos ou matéria que envolva cenas de nudez ou de atos sexuais de caráter privado quando são diretamente denunciados pelo participante ou seu representante legal, como está contido no art. 21 da lei em questão[119].

Apesar do Marco Civil da Internet, não regulamentar todas as áreas da responsabilidade civil no que concerne o espaço cibernético e seus usuários, o mesmo veio a beneficiar o ordenamento jurídico[120]. Em relação à matéria penal, falaremos agora da Lei nº 12.737 de 2012 que surgiu no ordenamento jurídico por impulso de uma circunstancia externa e promoveu alterações no código penal brasileiro. No ano de 2011 a atriz brasileira Carolina Dieckmann foi vítima de um golpe envolvendo o ambiente virtual, despertando mais uma vez o interesse da mídia a respeito dos crimes cibernético e consequentemente a sanção da lei que acabou por ficar conhecida com o seu nome.

Foi a partir de uma manutenção técnica, no computador da atriz, que um agente malicioso tomou posse de fotos íntimas da mesma, e através desta obtenção ilegítima, Carolina

---

[119] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 300.
[120] Ibidem, p. 278.

Dieckmann passou a ser vítima do crime de extorsão. Com isso ficou ainda mais evidente a falta de um dispositivo penal que tutelasse os dados informáticos, sendo esse o passo definitivo para a aprovação da lei que seguiu para sanção ou veto presidencial, nos seguintes moldes.

> Criou o delito de invasão de dispositivo informático simples (art. 154-A, CP);
> Criou uma figura assemelhada à da invasão simples de dispositivo informático, com mesma pena do *caput* para o partícipe do delito principal (ou praticante do delito de meio) impedindo sua punição em menor grau (art. 154-A, § 1°, CP);
> Criou uma causa de aumento específica para o delito de invasão simples em autoria ou participação, para o exaurimento com prejuízo econômico (art. 154-A, § 2°, CP);
> Criou uma modalidade qualificada de invasão de dispositivo informático (art. 154-A, § 3°, primeira parte, CP) pela obtenção de conteúdo sigiloso dos dados obtidos;
> Criou uma modalidade qualificada de invasão de dispositivo informático (art. 154-A, § 3°, segunda parte, CP) pela obtenção de controle remoto não autorizado;
> Criou uma causa de aumento específica para a invasão de dispositivo informático qualificada, com a divulgação, comercialização ou transmissão a terceiros dos dados obtidos;
> Criou uma causa de aumento geral para os delitos simples e qualificado pela especial qualidade da vítima imediata do delito (basicamente, altos cargos públicos).
> Determinou ser a ação penal pública condicionada a representação nos delitos com vítima comum e ação penal pública incondicionada, nos delitos com vítimas especiais, no que se refere aos delitos de invasão de dispositivo informático.
> Alterou o *nomen iuris* do delito do art. 266 do CP para "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", aumentando o rol dos crimes contra os serviços públicos;
> Acresceu o delito de interrupção ou perturbação de serviço informático, interrupção ou perturbação de serviço telemático e interrupção ou perturbação de informação de utilidade pública.
> Modificou o parágrafo da figura qualificada nos delitos de "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", visto que determina que seja dobrado a pena caso a conduta ocorra em circunstâncias de calamidade pública.
> Acresceu ao art. 298 um parágrafo único, com o *nomen iuris* de "falsidade de cartão", equiparando-se a documento particular o cartão de crédito ou de débito[121].

Nota-se que apenas ouve criação legislativa de um delito, qual seja, o delito de invasão de dispositivo informático, encontrados nos artigos 154-A e 154-B, ambos do Código Penal. No que diz respeito aos artigos 266 e 298, do mesmo dispositivo, estes apenas tiveram sua incidência alargadas, fazendo com que situações que antes não geravam consequências penais, por inexistência de previsão legal, agora passaram a ser criminalizada.

Então Analisando a inserção da Lei nº 12.737/12 nos artigos arts. 266 e 298 do Código Penal. Quanto ao art. 266, entende-se que, apesar de delito comum, que pode ser praticado por qualquer pessoa e tem como vítima a sociedade, compreende-se que em muitos casos se faz necessário elevada competência técnica para sua consumação.

É um tipo de crime que só acontece na sua forma dolosa, não sendo punido, por exemplo, o contágio involuntário de um sistema por vírus, mesmo este vindo a causar prejuízo,

[121] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 287.

pois não há tipicidade[122]. No que diz respeito à sanção, podemos dizer que não parecia como objetivo do legislador o encarceramento do delinquente, visto que a pena de 1 a 3 anos de detenção, imposta a esse delito, caberá ao infrator, desde que cumprido determinados requisito que não serão citados aqui, pois não é o objetivo do nosso trabalho, a substituição da pena privativa de liberdade por pena restritiva de direitos.

No que se refere ao regime inicial, caso não haja a substituição do encarceramento, o agente poderá iniciar no regime semiaberto ou aberto, a depender do entendimento do magistrado[123].

Analisando o art. 298 do dispositivo supracitado, foi incorporado a este o cartão de crédito e de débito como uma das definições de documento particular. Quanto à aplicação do Código Penal no tratamento do delito contido neste artigo, se dará quando houver a existência da produção de cartões falsos, adulteração de numeração, data de validade, entre outros. Costumeiramente apelidado de "dinheiro de plástico", o delito que envolva o cartão de crédito, nos faz questionar a possibilidade do seu enquadramento no crime de moeda falsa ao invés de falsificação de documento[124].

No que diz respeito ao artigo 154-A, invasão de dispositivo informático, este foi criado com a intenção de proteger a confidencialidade dos arquivos existentes nos dispositivos informáticos, porém foi inserido, de forma inadequada, no Capítulo VI, Dos Delitos contra a liberdade individual, na seção IV, Dos crimes contra a inviolabilidade de segredo, pois não somente dados profissionais merecem a Proteção Jurídica Penal, mas sim quaisquer dados existentes em dispositivo informático, sejam eles profissionais ou pessoais.

De acordo com o caput, para que haja a configuração desse delito serão necessários alguns requisitos. Em primeiro lugar que exista uma invasão ou tentativa de invasão a um dispositivo informático, sendo assim o acesso autorizado, mesmo que venha a destruir dados, não se enquadrará no referido artigo. Além do ingresso desautorizado, também precisa haver um objetivo específico, malicioso por parte do autor, pois não tipifica a conduta o mero ingresso desautorizado sem que haja a intenção de corromper, fraudar ou usurpar os dados de outrem.

Essa violação será feita a um dispositivo informático, estando este ligado ou não à rede de computadores, mas o que poderá ser enquadrado como sendo dispositivo informático?

---

[122] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 290.
[123] Ibidem, p. 292.
[124] Ibidem, p. 294.

Pois não houve por parte do legislador a definição, deixando em aberto o entendimento[125]. Sendo assim, e seguindo o senso comum, dispositivo informático é todo e qualquer equipamento eletrônico capaz de armazenar e transmitir dados. Ficando excluídos deste entendimento, os equipamentos eletrônicos que não estejam aptos a realizar tarefas relacionadas à execução de dados, como por exemplo, um relógio automático. Por outro lado, enquadram-se perfeitamente neste patamar, aparelhos celulares, smartphones, computadores, tablets, pen drives, etc[126].

Questão relevante se dá a respeito do grau de acesso, pois este poderá ocorrer nas seguintes formas: o usuário poderá ter permissão para acesso total, permissão para acesso parcial ou negação para acesso, sendo assim a partir do momento que alguém tem apenas a permissão parcial e acessa os dados como se permissão total tivesse, este estará infringindo a norma. A partir do momento que se é dado ao agente autorização para acesso, não existirá mais o núcleo do tipo penal. A permissão para o acesso poderá ser dada de forma expressa ou tácita, como também poderá ser revogada a qualquer tempo, no entanto vale destacar que um ato de disponibilidade fará com que se anule o nível de ofensividade.

Caso importante a se tratar é a possibilidade de ser utilizado um dispositivo informático de propriedade do agente para violar dados alheios, pois sabemos que essa conduta é comum tendo em vista a existência de dispositivos on-line que dispensam a materialidade para arquivar os dados dos usuários, possibilitando com isso, que o agente de posse de máquina de sua propriedade, acesse dados de outrem hospedados em rede[127]. Será que este ato ficaria sem proteção jurídica, pois o artigo deixar bem claro que a violação se dará em dispositivo informático alheio?

Em se tratando da violação de dispositivo informático alheio com a finalidade de instalação de vulnerabilidade, para que através desta, seja possível obter vantagem ilícita da vítima. Neste caso, o legislador deixou em aberto, podendo a vantagem almejada pelo agente ser de cunho patrimonial, sexual, intelectual, etc. Porém, o questionamento encontrado aí, diz respeito a esta ligação que há entre o dispositivo informático alheio, a instalação de vulnerabilidade no dispositivo de segurança e o objetivo de se obter vantagem ilícita. Pergunta-se: Se esse dispositivo informático pertencer à pessoa do agente e através dele for tentado se obter vantagem ilícita de terceiro, sem que para isso seja necessário que se instale vulnerabilidade no sistema, ainda assim seria possível o enquadramento nesse artigo?

---

[125] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 298.
[126] Ibidem, p. 298.
[127] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 305.

Se para a obtenção desta vantagem ilícita não for necessário à instalação de vulnerabilidade na máquina da vítima, mas aproveitando-se de uma brecha na segurança do sistema, por exemplo, não se pode considerar que cometeu o delito do artigo 154-A? Nesse raciocínio, se a instalação da vulnerabilidade for promovida por um agente e a obtenção de vantagem ilícita for obtida por outro, qual dos agentes se encaixará nesse delito? Vemos que existem perguntas pendentes a respeito do que pode ou não ser acobertado por este dispositivo.

No que tange a figura equiparada do § 1° do art. 154-A: "§ 1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput". Essa figura acaba por equiparar o agente à pessoa que prestou auxílio material à invasão, acabando este por ficar na mesma categoria do verdadeiro autor do delito, pois não houve para o partícipe a possibilidade de pena reduzida, mas sim, esse será punido com a mesma carga penal do cometedor direto[128].

No parágrafo 3° do referido artigo, o legislador ao criar uma figura qualificada quando houver a invasão a conteúdo privado, segredo comercial ou industrial, informações sigilosas ou de controle remoto não autorizado, será tratado de forma qualificada com pena em patamares mínimos e máximos superiores a do caput, pois nesse caso a figura prevê um resultado específico para a invasão. Não será necessário que seja gerado um resultado danoso, mas apenas a sua invasão já será suficiente.

É evidente que o homem médio brasileiro possuidor de dispositivo informático, muitas das vezes não possui intimidade com a língua inglesa, linguagem esta comumente usada para os procedimentos telemáticos, com isso surge à questão, trata-se de invasão ou de um acesso autorizado, ainda que indiretamente, pois este usuário pode vir a ser levado a erro e acabar por dar consentimento de uso. Neste caso deve ser averiguado no caso concreto, se essa autorização está eivada de algum tipo de vício de consentimento, erro, dolo ou coação[129].

O parágrafo 4§ tratará da hipótese de haver divulgação, comercialização ou transmissão à terceiro do conteúdo tratado no parágrafo 3°, neste caso, a pena será aumentada de 1 a 2 terços. Por divulgação entendemos ser o ato de levar ao conhecimento do público essas informações, já a comercialização ocorre quando os dados são colocados no mercado mediante preço; quanto à transmissão, se dará no momento em que essas informações são reveladas, repassadas a um terceiro, sendo que este terceiro será apenas uma pessoa e não o público. Todas estas atitudes são causas de aumento de pena.

[128] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 309.
[129] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 318.

A invasão e a divulgação precisam ser feitas pela mesma pessoa? A causa de aumento apenas ocorrerá quando tanto a invasão quanto a divulgação forem cometidas pela mesma pessoa, pois não seria correto que alguém sofresse alterações na sua pena por conduta cometida por terceiro[130].

O artigo 154-B tratará da questão processual penal no que se referir ao artigo 154-A. Trata-se de crime que apenas se procede mediante representação, salvo se for cometido contra a administração publica direta ou indireta de qualquer dos poderes da União, Estado, Distrito Federal ou Município, ou ainda contra empresas concessionárias de serviço público. Sendo assim, nos casos dos particulares, por tratar-se de ação pública condicionada à representação, deverá ser exercida no prazo mínimo de seis meses, a contar do dia em que vier a sabe quem é o autor do crime, conforme o artigo 38 do Código de Processo Penal.

Esse tipo de crime, quando enquadrado na maior das penas, no caso a do § 3º permitirá a sua substituição por pena restritiva de direito, e consequentemente o regime de cumprimento inicial semiaberto ou aberto[131].

Neste tópico procuramos explanar de forma clara alguns artigos do Marco Civil da internet, deixando evidente que o mesmo trata-se de uma lei civil e que necessário se faz o seu estudo, pois está regulamenta a conduta dos usuários e provedores. Na sequência procurou-se fazer um entendimento da Lei nº 12.737/12, pois a mesma foi de grande contribuição para o Código Penal brasileiro ao regulamentar, na esfera penal, o uso da internet no brasil.

Vale salientar, que alguns comportamentos delitivos cometidos no ambiente virtual, podem ser enquadrados nos artigos do código penal, porém recentemente, algumas condutas específicas foram regulamentadas pela Lei nº 12.737/12, mas o que se falar dos atos criminosos cometidos virtualmente que fogem dos moldes possíveis de ser regulados por estes artigos? Estas, de certo, não poderão ficar sem punição, no entanto, isso nos mostra que um reexame no código penal, cuja criação ocorreu no ano de 1940, já devia ser feito, se levarmos em consideração que delitos virtuais eram algo inimaginável na época.

Por fim, finalizamos o entendimento do capítulo terceiro, reforçando a mensagem de que no contexto atual, em uma era de inovações tecnológicas, é de se esperar que o crime virtual, assim como é fruto desta tecnologia, naturalmente que o mesmo aperfeiçoe as suas técnicas e aumente a incidência no mesmo ritmo com o qual evolui a modernidade da civilização, porém essa não é uma desculpa para a existência dessas formas delitivas, mas sim, um alerta à sociedade acerca dos métodos de prevenção e combate.

---

[130] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015. p. 320.
[131] Ibidem, p. 324.

Esperamos que através deste trabalho seja possível levar o entendimento necessário à sociedade, de forma que esta contribuição possa ser útil, evitando a ocorrência de algum delito ou contribuindo na persecução do criminoso virtual.

CONSIDERAÇÕES FINAIS

O presente trabalho iniciou-se com a apresentação dos fatos históricos que marcaram o surgimento da era da informática, pois é notório que estes acontecimentos tiveram papel fundamental no avanço tecnológico que atualmente propicia a ocorrência dos crimes cibernéticos, nele foi mostrado desde a origem dos computadores, passando-se para a chegada da internet até o surgimento dos crimes cibernéticos.

Em seguida foi feito a análise das fragilidades do ambiente informático e verificou-se a existência de falhas técnicas, sendo estas responsáveis por grande parte dos delitos informáticos, essas falhas deixam brechas no sistema e proporciona que o indivíduo mal intencionado execute a ação desejada. Foram descritos vário tipos de ataques que possivelmente se valeria dessas fragilidades, e como novos avanços etnológicos influencia no aparecimento de novos crimes, sendo assim, chegou-se a conclusão de que a existência da fragilidade técnica não será é algo que rotineiramente tende a parecer, tendo em vista que novas possibilidades de ataques apareceram enquanto novas formas de combate vão surgindo, como em um verdadeiro jogo de gato e rato. Porém, algo preocupante diz respeito ao fator humano, pois é este uma peça fundamental no que tange a criminalidade informática, este é o alvo preferido dos agentes criminosos e de acordo com as pesquisas feitas através deste trabalho verificou-se como este muitas vezes coopera com o crime de forma direta ou indireta, ou seja, os indivíduos têm seu grau de responsabilidade na conclusão do delito, pois são estes que acabam por falta nos devidos cuidados proporcionando a ocorrência dos mesmos.

Foram apontados alguns crimes que podem ser praticados através do ambiente virtual, e suas modalidades foram divididas em crimes contra o patrimônio, crimes contra a honra e crimes contra a dignidade sexual, as formas como estes podem ocorrer e em seguida foi tratado o perfil da vítima e do autor. Quanto ao perfil das vítimas, mais uma vez foi mostrado a possibilidade que estas têm de participar no delito, como estas são escolhidas e os diversos tipos de vítimas, já o autor constatou-se que este ao passar do tempo foi adquirindo novas condutas, diferentes qualificação, modalidades de ataque e até nomenclaturas, deixando bem claro que o autor do delito atual, a depender do tipo de crime, poderá ser qualquer pessoa do povo que tenha a capacidade básica, ao que tange o entendimento da tecnologia.

As formas de prevenção dos delitos, também foram vistas e o objetivo de orientação acerca da cautela que deve ser tomada foi exposto de várias formas, inclusive indicando carti-

lhas e endereços eletrônicos onde há disponibilidade de material para quem queira mais entendimento quanto ao tema, assim como também foi expostos às formas mais utilizadas de ataque e suas formas de prevenção. As formas de ação foram abordadas em um capítulo específicos onde foram tratados os procedimentos que devem ser tomados caso alguém venha a ser vítima de um crime virtual, foram expostos de maneira clara e objetiva, indicando os procedimentos necessários, desde a coleta de provas e seu armazenamento até a forma e locais da realização da ocorrência, tudo isso cumprindo com o objetivo de levar uma orientação para o público em geral, para que através desta ação seja possível ajudar a combater e a prevenir o delito virtual.

Por fim foi mostrado o que o ordenamento jurídico tem a oferecer acerca de uma forma delitiva tão recente, analisando o Marco Civil da internet e sua forma de regulamentação dos provedores e dos usuários e a Lei nº 12.757/13 e as contribuições e alterações trazidas por esta ao Código Penal Brasileiro. No entanto, e apesar do pouco tempo de existência da tecnologia que deu ênfase aos crimes cibernéticos, é notório que o ordenamento jurídico brasileiro necessita de mais respaldo, pois a regulamentação acerca deste tema é insuficiente e percebe-se que há uma falta de especificação, do enquadramento exato do delito, porém, não é possível se falar que há um total abandono ao que se refere a estes crimes.

REFERÊNCIAS

AMOROSO, Danilo. **O Que é Computação em Nuvem**. Tecmundo. 13 de junho de 2012. Disponível em:< http://www.tecmundo.com.br/computacao-em-nuvem/738-o-que-e-computacao-em-nuvens-.htm>. Acesso em: 01/10/15.

ARAS, Vladimir. **Internet Legal: O Direito na Tecnologia da Informação**. 1. ed. Org. Omar Kaminski. Curitiba: Juruá, 2011.

BRASIL. **Tribunal de Justiça do Rio Grande do Sul**. Recurso Cível n°71005058870/RS. Relator: CACHAPUZ, Ana Cláudia, Publicado no DJ de 29/09/2014. Disponível em:<http://tj-rs.jusbrasil.com.br/jurisprudencia/142667010/recurso-civel-71005058870-rs>. Acesso em: 14/10/15.

BRIGS, Asa; BURKE, Peter. **Uma História Social da Mídia: De Gutenberg à Internet**. 2. ed. Rio de Janeiro: Jorge Zahar, 2006.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Brasport, 2014.

CENTRO DE ESTUDO E RESPOSTA PARA TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Total de incidentes reportado ao CERT.br por ano. Disponível em:<http://www.cert.br/stats/incidentes/>. Acesso em: 06/10/15.

COMBATE A PORNOGRAFIA INFANTIL CUMPRE MANDADOS EM 3 CIDADES. Disponível em:<http://g1.globo.com/rn/rio-grande-do-norte/noticia/2015/09/combate-pornografia-infantil-cumpre-mandados-em-3-cidades-do-rn.html>. Acesso em: 05/09/15.

COMPUTER HISTORY MUSEUM. Disponível em:<http://www.computerhistory.org/revolution/personal-computers/17/297>.Acesso em: 03/06/15.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** São Paulo: Saraiva. 2000.

ESTUDO DO MERCADO BRASILEIRO DE SOFTWARE E SERVIÇOS 2015. p. 8. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** São Paulo: Saraiva. 2000. Estudo do Mercado Brasileiro de Software e Serviços 2015. p. 10. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

DELEGACIA PELA INTERNET. Disponível em: <http://servicos.sds.pe.gov.br/delegacia/> Acesso em: 22/10/2015.

DIGI DENÚNCIA. Disponível em: http://www.prsp.mpf.gov.br/noticias-prsp/aplicativos/digi-denuncia. Acesso em: 23/10/2015.

ESTUDO DO MERCADO BRASILEIRO DE SOFTWARE E SERVIÇOS 2015. p. 1. Disponível em:< http://www.abessoftware.com.br/dados-do-setor/dados-2014>. Acesso em: 02/06/15.

FERREIRA Ivette Senise. **Direito e Internet: Aspectos Jurídicos Relevantes**. 2. ed. Coord. Newton de Lucca; Adalberto Simão Filho e outros. São Paulo: Quartier Latin,2005.

FERREIRA, Érica Lourenço de Lima. **Internet: Macrocriminalidade e Jurisdição Internacional.** Curitiba: Juruá, 2007.

FONSECA FILHO, Cléuzio. **História da Computação: O Caminho do Pensamento e da Tecnologia.** Porto Alegre : Edipucrs, 2007.

GOLPE DO BOLETO FALSO NA INTERNET FAZ CADA VEZ MAIS VÍTIMAS NO PAÍS. Disponível em:<http://g1.globo.com/jornal-nacional/noticia/2015/05/golpe-do-boleto-falso-na-internet-faz-cada-vez-mais-vitimas-no-pais.html>. Acesso em: 25/08/15.

GRECO, Rogério. **Código Penal Comentado**. 4. ed. Niterói: Impetus, 2010.

KLEINA, Nilton. **Colossus: herói da guerra e um dos primeiros computadores do mundo**. Tecmundo, 14 de junho de 2013. Disponível em:<http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 02/06/15.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. 2. ed. São Paulo: Atlas, 2011.

LISTA DE PESQUISAS QUANTITATIVAS DE CONTRATOS ATUAIS. Disponível em: <http://www.secom.gov.br/atuacao/pesquisa/lista-de-pesquisas-quantitativas-e-

qualitativas-de-contratos-atuais/pesquisa-brasileira-de-midia-pbm-2015.pdf/view>. Acesso em: 01/06/15.

MENNA, Ricardo de Macedo B. **Direito e Redes Sociais na Internet: A Proteção do Consumidor no Comércio Eletrônico.** 2. ed. Curitiba: Juruá, 2014.

MERCADO BRASILEIRO DE SOFTWARE: PANORAMA E TENDÊNCIAS. 1. ed. São Paulo: ABES - Associação Brasileira das Empresas de Software, 2015. Disponível em: < http://central.abessoftware.com.br/Content/UploadedFiles/Arquivos/Dados%202011/ABES-Publicacao-Mercado-2015-digital.pdf> acesso em: 02/06/15.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar – Ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Education, 2003.

MORIMOTO, Carlos E. **O Apple 1: Guia do Hardware**. 04 de agosto de 2011. Disponível em < http://www.hardware.com.br/guias/historia-informatica/apple.html>. Acesso em: 04/06/15.

MORIMOTO, Carlos E. **O Lisa e o Macintosh: Guia do hardware**. 10 de agosto de 2011. Disponível em <http://www.hardware.com.br/guias/historia-informatica/lisa-macintosh.html>. Acesso em: 04/06/15.

MORIMOTO, Carlos E. **O Surgimento dos Computadores Pessoais**. Guia do hardware. 01 de janeiro de 2002. Disponível em: <http://www.hardware.com.br/livros/hardware-manual/surgimento-dos-computadores-pessoais.html>. Acesso em: 03/06/15.

MUSEU DO COMPUTADOR Universidade Estadual de Maringá. Disponível em: < http://www.din.uem.br/museu/hist_nobrasil.htm>. Acesso em: 02/06/15.

NO BRASIL 16 DOS PCS TEM PROTEÇÃO ZERO CONTRA AMEAÇAS, DIZ ESTUDOS. Disponível em: <http://www.crimespelainternet.com.br/no-brasil-16-dos-pcs-tem-protecao-zero-contra-ameacas-diz-estudo/>. Acesso em: 19/10/15.

PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO REALIZADA EM 2014 POR A EMPRESA DARYUS. DARYUS Group Brazil: Public Copyright 2014. Disponível em: < http://www.daryus.com.br/view/pdf/DARYUS_Pesquisa_ISM.pdf>. Acesso em: 13/07/2015.

RECLAME AQUI. Disponível em: http://www.reclameaqui.com.br/. Acesso em: 23/10/2015.

SAFERNET BRASIL. Disponível em: http://new.safernet.org.br/. Acesso em: 23/10/2015.

SILVA, Mauro Marcelo de Lima. **Internet Legal: O Direito na Tecnologia da Informação**. 1. ed. Org. Omar Kaminski. Curitiba: Juruá, 2011.

SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas**. 2 ed. São Paulo: Saraiva, 2015.

VÍRUS INTERROMPE SERVIÇO DO DETRAN-PE. São Paulo: Portal de Notícias G1. 06/02/2009. Disponível em: <http://g1.globo.com/Noticias/Brasil/0,,MUL990097-5598,00-VIUS+INTERROMPE+SERVICOS+PRESTADOS+PELO+DETRAN+EM+PERNAMBUCO.html>. Acesso em: 01/7/15