UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI
FACULDADE DE CIÊNCIAS EXATAS
CURSO DE SISTEMAS DE INFORMAÇÃO

CRIMES CIBERNÉTICOS: estudo de caso sobre crimes contra o patrimônio no âmbito da Internet à luz do Ordenamento Jurídico Brasileiro

Tamires Aylana de Medeiros Santos

Diamantina

2019

UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI
FACULDADE DE CIÊNCIAS EXATAS

CRIMES CIBERNÉTICOS: estudo de caso sobre crimes contra o patrimônio no âmbito da Internet à luz do Ordenamento Jurídico Brasileiro

Tamires Aylana de Medeiros Santos

Orientador(a):

Prof. Me. Erinaldo Barbosa da Silva

Trabalho de Conclusão de Curso apresentado ao Curso de Sistemas de Informação, como parte dos requisitos exigidos para a conclusão do curso.

Diamantina

2019

Santos, Tamires Aylana de Medeiros.
Crimes Cibernéticos: estudo de caso sobre crimes contra o patrimônio no âmbito da Internet à luz do Ordenamento Jurídico Brasileiro / Tamires Aylana de Medeiros Santos - 2019.
50.p

1. Crime Virtual 1; 2. Crime contra Patrimônio; 3. Marco Civil da Internet; 4. Lei Carolina Dieckmann I. Título.

CDU xxx.xx

CRIMES CIBERNÉTICOS: estudo de caso sobre crimes contra o patrimônio no âmbito da Internet à luz do Ordenamento Jurídico Brasileiro

Tamires Aylana de Medeiros Santos

Orientador(a):

Prof. Me. Erinaldo Barbosa da Silva

Trabalho de Conclusão de Curso apresentado ao Curso de Sistemas de Informação, como parte dos requisitos exigidos para a conclusão do curso.

APROVADO em ____ / ____ / _____.

_____

Prof. Me. Harley Fernandes de Almeida – UEMG

_____

Prof. Me. Rafael Santin – UFVJM

_____

Prof. Me. Erinaldo Barbosa da Silva – UFVJM

AGRADECIMENTO

Agradeço primeiramente a Deus por estar ao meu lado durante minha trajetória e por ter me concedido a oportunidade de finalizar mais uma etapa de minha vida com êxito. Aos meus pais e irmãos que me incentivaram e me apoiaram em inúmeros momentos desta jornada. Agradeço também a todos os meus amigos de curso que me ajudaram ao compartilhar os seus conhecimentos adquiridos, que de alguma forma, me fizeram ter ânimo para que o objetivo fosse cumprido. Agradeço em especial os meus amigos, Ramon Rocha Leite e Tommaso Bellone , que por inúmeras vezes me auxiliaram de diversas maneiras e desempenharam um excelente trabalho em equipe durante todo o curso. Deixo também meu agradecimento a todos os professores, por me orientarem e repassarem seus conhecimentos de forma singular. Em especial, agradeço ao meu orientador, Erinaldo Barbosa da Silva, pela paciência ao me orientar em meio as minhas oportunidades e realizações profissionais adversas.

RESUMO

O presente trabalho objetiva abordar a problemática dos crimes virtuais sob a ótica do Ordenamento Jurídico Brasileiro e realizar uma breve análise didática a respeito destes crimes. O enfoque do presente estudo são os crimes contra o patrimônio, em razão de sua importância e grande ocorrência no Brasil, buscando respaldo legal no Código Penal e leis Nº 12.965/14 - Marco Civil da Internet e Nº 12.737/12 - Lei Carolina Dieckmann. Inicia-se o trabalho com a Evolução dos Computadores e história da Internet antes de introduzir os conceitos e histórico dos Crimes Cibernéticos e dados estatísticos sobre a Criminalidade Cibernética. O trabalho visa, por fim, além de esclarecer sobre o tema, orientar a sociedade e os leitores deste trabalho sobre os riscos e crimes que estão sujeitos no ambiente virtual, além da dificuldade do Ordenamento Jurídico Brasileiro em acompanhar de maneira rápida como os crimes surgem na sociedade contemporânea.

Palavras-chave: Crime Virtual, Crime contra Patrimônio, Marco Civil da Internet, Lei Carolina Dieckmann.

ABSTRACT

The present work aims to address the problem of virtual crimes from the point of view of the Brazilian Legal Order and conduct a brief didactic analysis regarding these crimes. The focus of the present study is crimes against property, due to their importance and great occurrence in Brazil, seeking legal support in the Criminal Code and Laws No. 12.965 / 14 - Civil Registry and No. 12.737 / 12 - Carolina Dieckmann Law. Work begins on the Evolution of Computers and the history of the Internet before introducing the concepts and history of Cyber Crimes and statistical data on Cyber Crime. The purpose of this paper is to clarify the subject and guide the society and the readers of this work about the risks and crimes that are subject in the virtual environment, as well as the difficulty of the Brazilian Legal System in quickly following how crimes arise in contemporary society.

Keywords: Virtual Crime, Crime against Patrimony, Civil Landmark of the Internet, Carolina Dieckmann Law.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

De acordo com Almeida et al. (2015 apud SILVA, 2003, p.19), Cibernética é a "ciência geral dos sistemas informantes e, particularmente, dos sistemas de informação". Ou pode-se definir também que: "A Cibernética é uma tentativa de compreender a comunicação e o controle de máquinas, seres vivos e grupos sociais por meio de analogias com as máquinas eletrônicas" (CHAVES, 2015).

Almeida et al. (2015 apud SCHMIDT, 2014) enriquece a conceituação do crime de informática ao dizer que o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão. Logo, o 'Crime de Informática' pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los.

Sob uma perspectiva baseada na "Convenção sobre o Cibercrime de Budapeste", realizada no ano de 2001, entende-se que os crimes de informática são aqueles perpetrados por meio dos computadores, contra eles ou através deles, de modo que a maioria dos crimes é praticada por meio do sistema de internet (SCHMIDT, 2014 apud CASTRO, 2003).

Com a modernização das tecnologias a internet ao trazer benefícios para a sociedade, trouxe consigo também malefícios que assolam o cotidiano e que têm se tornando cada vez mais comum com o passar dos dias. Sendo assim, o uso cotidiano da internet não têm sido, há muitos anos, mais um meio para passar o tempo, mas sim, para obter conhecimentos, realizar uma transação bancária, comprar algum produto, realizar eventos e/ou ter um perfil profissional em redes sociais, por exemplo.

Em se tratando das empresas, a rede é utilizada para auxiliar na tomada de decisões, divulgar seu produto, atrair clientes, interagir com seus consumidores, negociar com parceiros de empreendimento, além da utilização de redes sociais como plataforma de suporte para os negócios. Ou seja, pode-se dizer que o uso da rede de computadores e o uso da internet é uma necessidade individual e profissional para as empresas.

Todavia, essa comodidade virtual, sem a mobilização e conscientização correta para seu uso, abriu as portas para o cometimento dos crimes virtuais, na medida em que os métodos de propagação e transferência de dados avançaram. Sendo assim, há restrita preocupação de atribuir, junto a este avanço, um método preventivo voltado a segurança dos usuários, dados, informações e empresas.

Nota-se que a relação da internet com os crimes patrimoniais está no avanço da internet e sua evidente dependência no cotidiano dos indivíduos.Nota-se também que os crimes virtuais contra o patrimônio cresce paralelamente a isto.

Neste estudo o enfoque será dado para os crimes contra patrimônio uma vez que estes têm índices cada vez mais crescentes nos Estados Brasileiros e por serem diversos, em se tratando da forma como podem ser praticados e enquadrados pelo Código Penal e demais Leis previstas e citadas neste trabalho.

2 DESENVOLVIMENTO

2.1 Introdução à Evolução dos Computadores

Não há como falar em Crimes Cibernéticos sem antes passar por uma apresentação dos aspectos mais relevantes no que diz respeito ao histórico da invenção tanto do computador quanto da Internet. Afinal, é por meio deste instrumento que se envia, recebe dados e que a grande maioria dos Crimes Virtuais acontecem.

A área tecnológica é uma corrida contra o tempo em todos os sentidos. Tem-se a preocupação com obsolescência dos equipamentos, uma vez que a vida útil do equipamento diminui e com o passar do tempo tornam-se inutilizáveis para realizar determinadas tarefas e objetivos.

Sendo assim, a evolução tecnológica permitiu que os componentes dos equipamentos alcançassem uma alta escala de produção e oferecesse mercados melhores, com um preço mais satisfatório e acessível aos usuários de interesse. Esse preço diz respeito a além de valor do equipamento, gastos com requisitos instalações, fiação, entre outros.

Inicialmente, é importante destacar que, “existe uma enorme variedade de produtos que podem ser denominados computadores, desde microcomputadores baseados em uma única pastilha (chip), que custam poucos dólares, até supercomputadores, no valor de dezenas de milhões de dólares” (STALLINGS,2003).

Segundo Souza (2015), o computador nada mais é do que uma máquina eletrônica que possibilita o processamento de dados. Este termo é originário da palavra Latim *computare*, que significa “aquele que faz cômputos”, ou seja, que calcula.

Outra definição para computador é dada por Marçula e Filho (2005) “Computador é uma máquina que recebe e trabalha os dados de maneira a obter um resultado. Para realizar isso, ele é programável, ou seja, responde a um grupo de comandos específicos (instruções) de uma maneira bem definida e pode executar uma lista pré-gravada desses comandos. Esta lista é chamada de programa”.

Sucintamente, Manzano e Izabel (2007) definem como computador um conjunto de dispositivos eletrônicos interligados, os quais conseguem executar automaticamente um determinado trabalho, orientados por programa e em grande velocidade.

Em se tratando da história do computador, pode-se recordar alguns parâmetros de classificação existentes. A principal classificação existente dos equipamentos é quanto ao seu porte, levando-se em consideração o nível do potencial oferecido pela máquina.

Na visão de Jr e Azevedo (2000), "em função do potencial oferecido pelo equi-

pamento, ele recebe o título de equipamento de pequeno/ médio/ grande porte". Pode-se também classificá-los, segundo os autores, em função do potencial processamento, que são as capacidades de processamento (memórias, discos etc.), velocidade e quantidade de instruções do processador, condições de gerência de periféricos, resolução gráfica etc.

Em tempos anteriores, os equipamentos que permitiam certa aplicação mais pesada, mais profissional, eram os de maior porte. Esses equipamentos demandavam grande investimento de recursos e o custo era elevado para o usuário; isto tanto em termos de software, hardware e *pleopleware* (recursos humanos, treinamento, reciclagem/ atualização etc.)" (JR; AZEVEDO, 2000).

Sabe-se que, nos dias atuais, o equipamento ter o porte ou tamanho maior não significa ser mais robusto, profissional ou tecnológico necessariamente que os de menor porte, devido ao fato do esforço e investimento em reduzir o tamanho da máquina e ao mesmo tempo se obter um desempenho maior ou tão bom quanto ao citado anteriormente.

Segundo STALLINGS (2002) "Um dos fatores responsáveis pelo grande aumento da velocidade dos processadores é a diminuição do tamanho dos componentes dos microprocessadores; isso acarreta a redução da distância entre os componentes e, consequentemente, o aumento da velocidade."

De acordo com STALLINGS (2003), é comum classificar os computadores em gerações, de acordo com a tecnologia básica de hardware empregada. Cada nova geração é caracterizada por computadores com maior velocidade, maior capacidade de memória e menor tamanho que os computadores da geração anterior. Tanenbaum (2007) e Stallings e Midorikawa (2002) discorrem a respeito dos principais marcos no desenvolvimento histórico, de forma a entender sobre como ocorreu o processo até se desmembrar na evolução atual.

1. A Geração Zero - Computadores Mecânicos (1642-1945)

   A primeira pessoa a construir uma máquina de calcular operacional foi o cientista francês Blaise Pascal (1623-1662), em honra de quem a linguagem Pascal foi batizada. Esse dispositivo, construído em 1642, foi projetado para auxiliar seu pai, um coletor de impostos do governo francês. Era inteiramente mecânico, usava engrenagens e funcionava com uma manivela à mão.

   A máquina de Pascal podia efetuar apenas operações de adição e subtração. Mais de 30 anos mais tarde o grande matemático alemão, barão Gottfried Wilhelm von Leibniz (1646-1716), construiu uma outra máquina mecânica que também podia multiplica e dividir. Na verdade, Leibniz construiu o equivalente a uma calculadora de bolso no época.

Em 1792, um professor de matemática da Universidade de Combrigde, Charles Babbage, o inventor do velocímetro, projetou e construiu sua primeira máquina diferencial. A máquina diferencial era um dispositivo mecânico que, assim como o de Pascal, só podia somar e subtrair, ela foi projetada para calcular tabelas de números úteis para a navegação naval. Interessante era o método de saída da máquina: ela perfurava seus resultados sobre uma chapa de gravação de cobre, prenunciando futuros meios de escrita única como cartões perfurados e CD.

2. A Primeira Geração - Válvulas Eletrônicas (1945-1955)

   O ENIAC (Computador e Integrador Numérico Eletrônico - Eletronic Numerical Integrator and Computer), projetado e construído sob a supervisão de John Mauchly e John Presper Eckert na Universidade da Pensilvânia, foi o primeiro computador eletrônico digital de propósito geral em todo mundo. O projeto foi uma resposta as necessidades dos Estados Unidos diante da Segunda Guerra Mundial. O laboratório de Pesquisas Balísticas do Exército Americano(Army's Ballistics Research Laboratory- BRL), órgão responsável por desenvolver tabelas com boa precisão e em tempo hábil, senão a artilharia seria inútil. O BRL utilizava calculadoras de mesa que consumia horas ou até dias de trabalho de uma pessoa. Então, um professor de Engenharia Elétrica juntamente com seu aluno de pós-graduação, propuseram a construção de um computador de propósito geral para as aplicações do BRL, utilizando válvulas. Em 1943, a proposta foi aceita pela Exército Americano e o trabalho no ENIAC teve início.

   O resultado foi uma máquina que pesava 30 toneladas, ocupava espaço de aproximadamente 140 metros quadrados e continha mais de 18 mil válvulas. A operação da máquina consumia 140 quilowatts de energia elétrica.

3. A Segunda Geração - Transistores (1955-1965)

   A primeira grande mudança nos computadores eletrônicos veio com a substituição da válvula pelo transistor. O transistor é menor, mais barato e dissipa menos calor do que a válvula e, assim como a válvula, também pode ser utilizado para a construção de computadores. Ao contrário da válvula, que requer o uso de fios, placas de metal, cápsula de vidro e vácuo, o transistor é um dispositivo de estado sólido, feito de silício.

4. A Terceira Geração - Circuitos Integrados (1965-1980)

   Os computadores do início da segunda continham cerca de 10 mil transistores, esse número cresceu até centenas de milhares. Em 1958, foi desenvolvida uma nova téc-

nica que revolucionou os equipamentos eletrônicos e iniciou a era da microeletrônica: a invenção do circuito integrado.

5. Últimas gerações

   A partir da terceira geração de computadores, existe menos consenso sobre a definição das demais gerações de computadores. O Quadro 1 sugere a existência de uma quarta e quinta gerações, com base na evolução da tecnologia de circuitos integrados.

Quadro 1: Gerações de computadores

Geração	Datas aproximadas	Tecnologia	Velocidade típica (operações por segundo)
1	1946-1957	Válvula	40.000
2	1958-1964	Transistor	200.000
3	1965-1971	Integração em baixa e média escalas	1.000.000
4	1972-1977	Integração em grande escala	10.000.000
5	1978	Integração em escala muito grande	100.000.000

Fonte: (STALLINGS; MIDORIKAWA, 2002, p. 28).

De acordo com Stallings e Midorikawa (2002), com a introdução de integração em grande escala, mais de mil componentes podem ser colocados em uma única pastilha de circuito integrado. A integração em escala muito grande atingiu mais de 10 mil componentes por pastilha, e as pastilhas atuais podem conter mais de cem mil componentes.

Sendo assim, com o rápido avanço da tecnologia, a introdução significativa de novos produtos e a importância do software e das comunicações, tanto quanto do hardware, a classificação em gerações torna-se menos significativa.

O Quadro 2 lista alguns marcos do desenvolvimento do computador digital moderno, com seus respectivos anos, nomes, quem o constituiu e cometário.

Quadro 2: Alguns marcos do desenvolvimento do computador digital moderno

Ano	Nome	Construído por	Comentários
1834	Máquina analítica	Babbage	Primeira tentativa de construir um computador digital
1936	Z1	Zuse	Primeira máquina de calcular com relés
1943	COLOSSUS	Governo Britânico	Primeiro computador eletrônico
1944	Marki	Aiken	Primeiro computador norte-americano de uso geral
1946	ENIAC	Eckert/ Mauchley	A história moderna dos computadores começa aqui
1949	EDSAC	Wilkes	Primeiro computador com programa armazenado
1951	Whirlwind I	M.I.T	Primeiro computador de tempo real
1952	IAS	von Neumann	A maioria das máquinas atuais usa esse projeto
1960	PDP-1	DEC	Primeiro microcomputador (50 vendidos)
1961	1401	IBM	Máquina para pequenos negócios de enorme popularidade
1962	7094	IBM	Dominou a computação científica no início da década de 1960
1963	B5000	Burroughs	Primeira máquina projetada para uma linguagem de alto nível
1964	360	IBM	Primeira linha de produto projetada como uma família
1964	6600	CDC	Primeiro super computador científico
1965	PDP-8	DEC	Primeiro minicomputador de mercado de massa (50 mil vendidos)
1970	PDP-11	DEC	Dominou os minicomputadores na década de 1970
1974	8080	Intel	Primeiro computador de uso geral de 8 bits em um chip
1974	CRAY-1	Cray	Primeiro supercomputador vetorial

1978	VAX	DEC	Primeiro superminicomputador de 32 bits
1981	IBM PC	IBM	Deu início à era moderna do computador pessoal
1981	Osborne-1	Osborne	Primeiro computador portátil
1983	Lisa	Apple	Primeiro computador pessoal com uma GUI
1985	386	Intel	Primeiro ancestral de 32 bits da linha Pentium
1985	MIPS	MIPS	Primeira máquina comercial RISC
1987	SPARC	Sun	Primeira estação de trabalho RISC baseada em SPARC
1990	Rs6000	IBM	Primeira máquina superescalar
1992	Alpha	DEC	Primeiro computador pessoal de 64 bits

Fonte: (TANENBAUM, 2007).

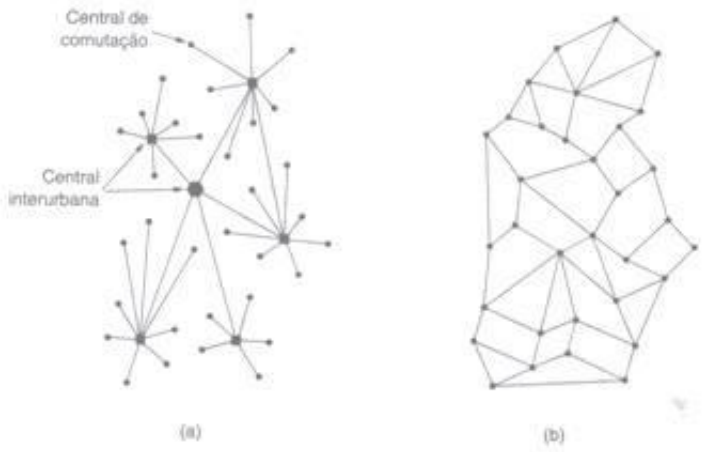
2.2 História da Internet

Antes de entender o contexto histórico em que a Internet surgiu e sua evolução, é importante mencionar o seu conceito e algumas definições relacionadas a ela, a fim de que seja possível o melhor entendimento do trabalho. Afinal, apesar de a maioria das pessoas saberem os benefícios trazidos a partir do seu uso, muitas vezes não sabem precisamente o seu conceito. Tem-se algumas definições do conceito de Internet a partir da visão de alguns autores:

Segundo Tanembaum (2003), a Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns.

A história da Internet começa no final da década de 1950, no auge da Guerra Fria, quando o Departamento de Defesa dos Estados Unidos queria uma rede de controle e comando capaz de sobreviver a uma guerra nuclear. Nessa época, segundo Tanembaum (2003), “todas as comunicações militares passavam pela rede de telefonia pública, considerada vulnerável”, ou seja, necessitava-se de uma rede que não fosse tão centralizada como era a estrutura do sistema de telefonia na época, como mostra a Figura 1:

Figura 1: (a) Estrutura do sistema de telefonia (b) Sistema distribuído de comutação



Fonte: (TANEMBAUM, 2003).

Percebe-se na figura anterior que, segundo Tanembaum (2003, p.54), “os pontos pretos representam centrais de comutação telefônica que por sua vez são conectadas a milhares de telefones. Estas centrais de comutação telefônica estavam conectadas a centrais de comutação de nível mais alto (centrais interurbanas), formando uma hierarquia nacional.”

Percebe-se que a vulnerabilidade do sistema está no fato de que a destruição de alguma central interurbana poderia deixar o sistema isolado. Logo, não haveria mais comunicação durante a Guerra Nuclear.

3 CRIMES CIBERNÉTICOS

3.1 Conceitos e histórico dos Crimes Cibernéticos

Para entender o que é um crime cibernético é preciso primeiramente entender o conceito de crime segundo a Legislação Brasileira. Segundo o art. 1º da Lei de Introdução do Código Penal (decreto-lei nº 2.848, de 7/12/1940):

> "Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativamente ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente."

Ou seja, pela ótica da legislação brasileira, crime é qualquer infração em que a lei enseja pena de reclusão ou de detenção, que pode ser alternativa ou cumulativamente com pena de multa.

O delito cometido por meio da rede mundial, com o auxílio de computador, é denominado Crime Cibernético. De uma forma ampla, o Departamento de Justiça dos Estados Unidos define o crime cibernético como "quaisquer violações de leis criminais que envolvam, para sua perpetração, investigação ou persecução, o conhecimento de tecnologia de computador". Assim, tal como a criminalidade habitual, pode ocorrer em diversos locais, a qualquer momento.

Pode-se ressaltar que os criminosos utilizam-se de suas aptidões e conhecimentos específicos, desenvolvendo os mais variados métodos para alcançarem seus objetivos, englobando uma gama muito ampla de ataques.

Em se tratando da Symantec, empresa especializada em segurança de computadores, proteção de dados e software de gerenciamento remoto, conhecida graças ao antivírus "Norton", baseada em diversas definições de crime cibernético, esta o define como qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de hardware.

O conceito de Crimes Cibernéticos, também conhecidos como Cibercrimes, crimes virtuais, crimes da informática, crimes informáticos, é muito amplo e tem as mais variadas descrições. Uma acepção muito ampla de Crimes Cibernéticos é dada por Ferreira (2005, p.54)

> "As várias possibilidades de ação criminosa na área de informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, dos processamentos e transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um dominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores."

Historicamente, o termo "Cibercrime" surgiu após uma reunião, em Lyon, na França, de um subgrupo das nações do G8 (Estados Unidos, Japão, Alemanha, Reino

Unido, França, Itália, Canadá e Rússia), para estudar os problemas da criminalidade então causados via aparelhos eletrônicos ou pela disseminação de informações para a internet. Este "Grupo de Lyon" empregava o termo para descrever, de forma muito vasta, todos os tipos de crime praticados na Internet (PERRIN, 2006).

São exemplos de crimes que podem admitir sua execução no meio cibernético: crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (COLARES, 2002).

Quanto a criminalidade cibernética e uma lei especial regente, pode-se dizer que com a prática crescente de tais delitos, torna-se uma necessidade a sua repreensão, através de parcerias de autoridades especialistas das áreas de Computação e do Direito juntamente com a sociedade, a fim de que tais crimes sejam fiscalizados, buscando, com isso, uma conscientização dos usuários da rede de computadores.

É importante ressaltar que as dificuldades de identificação e controle de usuários, bem como as controvérsias sobre a produção de provas baseadas em fontes cibernéticas, são fatores que estabelecem barreiras no combate a esses crimes. Dentre as práticas criminosas mais comuns, podemos listar: furto de dados, estelionato, clonagem de cartões, injúria, calúnia, difamação, apologia ao racismo, homofobia, pedofilia, vandalismo informático (*cyberpunk*) e o terrorismo (DADALTI, 2009).

3.2 Criminalidade na Rede

- Do Patrimônio

De acordo com Marcondes (2017) os crimes contra o Patrimônio são aqueles que atentam diretamente contra o patrimônio de uma pessoa ou organização. Considera-se patrimônio de uma pessoa física ou organização, os bens, o poderio econômico, a universalidade de direitos que tenham expressão econômica para seu proprietário. O Patrimônio é um complexo de bens que serve para satisfazer necessidades pessoais e organizacionais.

As organizações empresariais, para protegerem seu patrimônio contra ações criminosas, adotam medidas de segurança patrimonial. A segurança patrimonial pode ser

compreendida como um conjunto de atividades do ramo da segurança privada, que tem como objetivo prevenir e reduzir perdas patrimoniais.

- Dos Crimes

O professor Paulo Sumariva, delegado de Polícia, doutor em Direito e professor da LFG, diz que quando os crimes contra o patrimônio são retratados, é importante focar o estudo nos crimes comuns como, por exemplo, os diferentes tipos de furto (LFG, 2017). Segue a descrição de forma sucinta os principais crimes contra o Patrimônio e as penas aplicáveis que estão previstas no Código Penal Brasileiro - Decreto Lei 2.848, de 7 de Dezembro de 1940.

Segundo o Código Penal e esclarecimentos de Luz (2017), tem-se como crimes contra o Patrimônio:

DOS CRIMES CONTRA O PATRIMÔNIO - DO FURTO

Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:

Pena - reclusão, de um a quatro anos, e multa.

§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.

§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico. O furto é a apropriação indevida de uma coisa alheia para si mesmo com o fim de apoderar-se dela de modo definitivo. Ou seja, é quando o indivíduo toma para si algo que não é de seu pertence, com o desejo de tê-lo para si definitivamente ou passar adiante com a finalidade de lucrar.

Sobre as penas impostas aos acusados de furto, o IPEA (Instituto de Pesquisa Econômica e Alternativa) apresenta em uma de suas pesquisas realizadas em vários estados Brasileiros, que 20,70% das condenações aplicadas nos 1.394 processos analisados, resultaram em medida alternativa, os demais 79,03% forma sentenciados a prisão privativa da liberdade ou semiaberto ou aberto. Diferente de outros países como a Inglaterra que possuí uma porcentagem quase que comparativamente oposta, aonde apenas 21% de seus acusados cumprem a prisão de restrição de liberdade, sendo o resto sentenciados ao cumprimento de penas alternativas.

No Brasil o código penal permite que as penas alternativas sejam aplicadas a quem

cometer crimes com pena inferior a quatro anos, sendo que não tenha ocorrido violência ou grave ameaça à pessoa, ou em caso de crimes culposos.

Segundo o ABCTec (2017) roubo e furto formam juntos um índice de 32% da criminalidade existe e ocorrente hoje no Brasil, visando esse índice foi lançado recentemente um projeto de reforma do código penal, no qual, visa o estabelecimento de penas mais duras aos praticantes de tais ilícitos.

FURTO QUALIFICADO

§ 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;

III - com emprego de chave falsa;

IV - mediante concurso de duas ou mais pessoas.

§ 5º - A pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.

§ 6º A pena é de reclusão de 2 (dois) a 5 (cinco) anos se a subtração for de semovente domesticável de produção, ainda que abatido ou dividido em partes no local da subtração.

O § 4º do artigo 155 C.P. prevê inúmeras hipóteses em que se qualifica o crime de furto, cominando-se a pena de dois a oito anos de reclusão e multa. O inciso I refere-se à destruição ou rompimento de um obstáculo para se chegar até a coisa que ele deseja furtar. Nesta situação o agente pode inutilizar, desfazer, desmanchar, arrebentar todos os obstáculos.

O inciso II refere-se ao abuso de confiança que existe quando o agente aproveita do momento em que o sujeito passivo da menos proteção a coisa, diante da confiança depositada no agente. Fraude é um meio enganoso utilizado pelo agente para subtrair a coisa, pratica o crime de fraude quem por exemplo se passa falsamente por um funcionário de uma concessionária de serviços públicos, aquele que distrai o balconista para pegar uma coisa para ele poder subtrair outra, aquele que passa por convidado de uma festa para adentrar a residência.

A escalada é utilização de uma via anormal para adentrar a casa ou ao local para operar a subtração, neste caso o agente deve fazer o uso de escadas ou cordas. A destreza é a habilidade física ou manual do agente, um meio dessa qualificadora é a “punga” onde a subtração de dinheiro ou carteira em locais que tem aglomeração de muitas pessoas, outro

caso de destreza é quando a vítima esta distraída e o agente pratica a subtração.

O inciso III refere-se ao emprego de chave falsa, em que inclui a imitação da verdadeira e o instrumento que pode ser utilizado pelo agente para fazer funcionar o mecanismo de uma fechadura ou instrumento análogo.

DOS CRIMES CONTRA O PATRIMÔNIO - DO ROUBO E DA EXTORSÃO

ROUBO

Art. 157 - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência:

Pena - reclusão, de quatro a dez anos, e multa.

§ 1º - Na mesma pena incorre quem, logo depois de subtraída a coisa, emprega violência contra pessoa ou grave ameaça, a fim de assegurar a impunidade do crime ou a detenção da coisa para si ou para terceiro.

§ 2º - A pena aumenta-se de um terço até metade:

I - se a violência ou ameaça é exercida com emprego de arma;

II - se há o concurso de duas ou mais pessoas;

III - se a vítima está em serviço de transporte de valores e o agente conhece tal circunstância.

IV - se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior;

V - se o agente mantém a vítima em seu poder, restringindo sua liberdade.

§ 3º Se da violência resulta lesão corporal grave, a pena é de reclusão, de sete a quinze anos, além da multa; se resulta morte, a reclusão é de vinte a trinta anos, sem prejuízo da multa.

Roubo é a subtração de coisa alheia móvel, para si ou para outrem, que caracteriza o furto, quando revestida de circunstâncias especialmente relevantes previstas na lei. Trata-se de crime contra o patrimônio em que é atingida, também a integração física ou psíquica da vitima. Ou seja, se o agente estabelecer contato com a vítima, ou violência ou ameaça, além da apropriação indébita de algo que lhe pertence, se caracteriza um roubo, diferente do furto que é quando o agente pratica o ilícito mais não estabelece um contato com a vítima.

Segundo o Programa das Nações Unidas para o Desenvolvimento - Pnud, o Brasil possui a maior taxa de roubos da América Latina, foram analisados 18 países, entre eles Bolívia, Argentina, Uruguai (G1, 2013).

EXTORSÃO

Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:

Pena - reclusão, de quatro a dez anos, e multa.

§ 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade.

§ 2º - Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior.

§ 3o Se o crime é cometido mediante a restrição da liberdade da vítima, e essa condição é necessária para a obtenção da vantagem econômica, a pena é de reclusão, de 6 (seis) a 12 (doze) anos, além da multa; se resulta lesão corporal grave ou morte, aplicam-se as penas previstas no art. 159, §§ 2º e 3º, respectivamente.

EXTORSÃO MEDIANTE SEQUESTRO

Art. 159 - Sequestrar pessoa com o fim de obter, para si ou para outrem, qualquer vantagem, como condição ou preço do resgate.

Pena - reclusão, de oito a quinze anos.

§ 1o Se o sequestro dura mais de 24 (vinte e quatro) horas, se o sequestrado é menor de 18 (dezoito) ou maior de 60 (sessenta) anos, ou se o crime é cometido por bando ou quadrilha.

Pena - reclusão, de doze a vinte anos.

§ 2º - Se do fato resulta lesão corporal de natureza grave:

Pena - reclusão, de dezesseis a vinte e quatro anos.

§ 3º - Se resulta a morte

Pena - reclusão, de vinte e quatro a trinta anos.

§ 4º - Se o crime é cometido em concurso, o concorrente que o denunciar à autoridade, facilitando a libertação do sequestrado, terá sua pena reduzida de um a dois terços.

EXTORSÃO INDIRETA

Art. 160 - Exigir ou receber, como garantia de dívida, abusando da situação de alguém, documento que pode dar causa a procedimento criminal contra a vítima ou contra terceiro:

Pena - reclusão, de um a três anos, e multa.

DOS CRIMES CONTRA PATRIMÔNIO - DO DANO

DANO

Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção, de um a seis meses, ou multa.

DANO QUALIFICADO

Parágrafo único - Se o crime é cometido:

I - com violência à pessoa ou grave ameaça;

II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave;

III - contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos;

IV - por motivo egoístico ou com prejuízo considerável para a vítima:

Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Tem-se com exemplos: Destruir: perder totalmente o bem; exemplo - queimar um livro.

Inutilizar: fazer com que o objeto perca sua finalidade, exemplo - quebrar as hélices de um ventilador.

Deteriorar: quebrar um pedaço, mais o bem continua apto para exercer sua funções, exemplo - quebrar os vidros de um carro.

DOS CRIMES CONTRA O PATRIMÔNIO - DA APROPRIAÇÃO INDÉBITA

APROPRIAÇÃO INDÉBITA

Art. 168 - Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção:

Pena - reclusão, de um a quatro anos, e multa.

Aumento de pena

§ 1º - A pena é aumentada de um terço, quando o agente recebeu a coisa:

I - em depósito necessário;

II - na qualidade de tutor, curador, síndico, liquidatário, inventariante, testamenteiro ou depositário judicial;

III - em razão de ofício, emprego ou profissão.

DOS CRIMES CONTRA O PATRIMÔNIO - DO ESTELIONATO E OUTRAS FRAUDES

ESTELIONATO

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

§ 2º - Nas mesmas penas incorre quem:

Disposição de coisa alheia como própria

I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;

Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;

Defraudação de penhor

III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;

Fraude na entrega de coisa

IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;

Fraude para recebimento de indenização ou valor de seguro

V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;

Fraude no pagamento por meio de cheque

VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Fraude no comércio

Art. 175 - Enganar, no exercício de atividade comercial, o adquirente ou consumidor:

I - vendendo, como verdadeira ou perfeita, mercadoria falsificada ou deteriorada;

II - entregando uma mercadoria por outra:

Pena - detenção, de seis meses a dois anos, ou multa.

§ 1º - Alterar em obra que lhe é encomendada a qualidade ou o peso de metal ou substituir, no mesmo caso, pedra verdadeira por falsa ou por outra de menor valor; vender pedra falsa por verdadeira; vender, como precioso, metal de ou outra qualidade:

Pena - reclusão, de um a cinco anos, e multa.

§ 2º - É aplicável o disposto no art. 155, § 2º.

OUTRAS FRAUDES

Art. 176 - Tomar refeição em restaurante, alojar-se em hotel ou utilizar-se de meio de transporte sem dispor de recursos para efetuar o pagamento:

Pena - detenção, de quinze dias a dois meses, ou multa.

Parágrafo único - Somente se procede mediante representação, e o juiz pode, conforme as circunstâncias, deixar de aplicar a pena.

Baseado na explanação acima, pode-se concluir que furto, o roubo e o dano juntos, encontram-se hoje como uns dos maiores índices de ocorrências estatísticas no Brasil. Foi possível observar que o patrimônio, para efeitos penais, compreende não só bens de valor econômico, mas também aqueles de valor puramente moral e/ou afetivo.

Fica concluído também que crimes contra o patrimônio, em regra, são dolosos e, sendo dolosos, são quase sempre acompanhados por elementos subjetivos do tipo, como,

v.g., “para si ou para outrem”; “em proveito próprio ou de outrem” etc.

Os crimes de furto e roubo, que são crimes contra o Patrimônio, podem ocorrer através de sistemas informantes ou sistemas de informação. Pode-se afirmar que esta modalidade de crime pode ser cometida por meios de dispositivos virtuais, ou seja, o acesso a informação ou ao poderio econômico é evidentemente mais fácil, devido a falta de proteção dos dados ou pelo conhecimento de algum especialista em cometer este tipo de crime. Conclui-se que o cometimento dos crimes de furto e roubo estão notoriamente ligados com os Crimes Cibernéticos.

3.3 Dados Estatísticos

A Folha de São Paulo, no ano de 2017, publicou uma notícia com o seguinte título: “Crimes contra o Patrimônio fazem uma vítima em São Paulo a cada 30 segundos.” A epidemia de crimes patrimoniais vivida pela população de São Paulo e que fez uma vítima a cada três segundos no Estado é uma estatística dos primeiros 6 meses daquele ano. Entram nessa conta furtos, roubos e latrocínios (roubos com morte). De carro a celular, incluindo roubos a banco e roubos de carga. Enfim, crimes que envolvem algum bem de valor (PAGNAN; MARIANI, 2017).

Segundo o ABCTec (2016) partindo do princípio de que o comércio eletrônico mudou, e muito, a maneira como as pessoas transacionam, os consumidores têm hoje acesso praticamente ilimitado a mercadorias e serviços a um baixo custo, favorecidos pela distribuição desses bens em um mercado virtual não restrito a barreiras geográficas.

Pode-se concluir que os ataques e ameaças digitais estão cada vez mais sofisticadas o que cria um desafio crítico para a manutenção de níveis satisfatórios de proteção dos ambientes de Tecnologia de Informação.

Sabe-se que o custo cada vez menor de hardware, maior poder de processamento e desenvolvimento de técnicas complexas de exploração de falhas aumentam a complexidade dos incidentes.

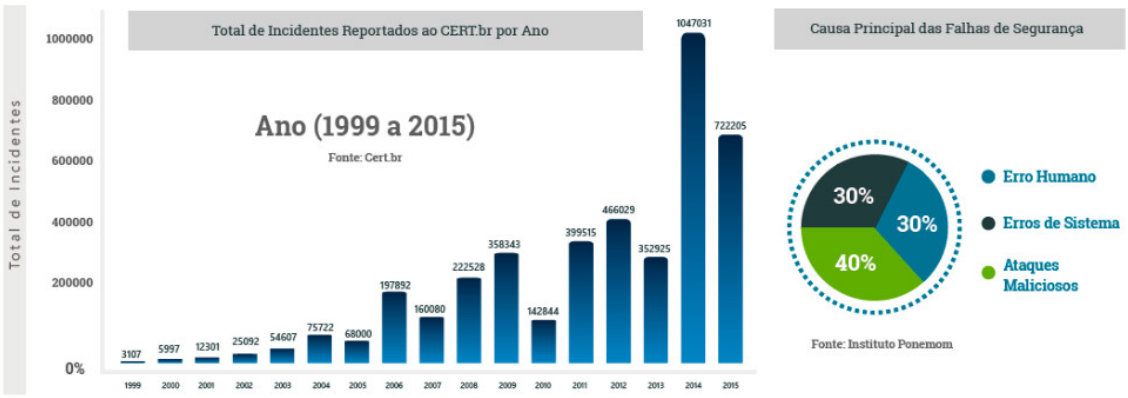
A ABCTec[1], Tecnologia em Segurança da Informação, divulgou gráficos com percentuais acerca das principais falhas de segurança e seus incidentes (FIG. 2).

Pode-se destacar que em menores proporções no que diz respeito as falhas de segurança estão o erro humano e os erros do sistema. Entretanto, 40/100 das falhas de segurança acorrem devido a ataques maliciosos, ou seja, foi utilizado programas, códigos ou condutas especificamente com a intenção de executar ações danosas e atividades

[1] ABCTec: empresa Brasileira que presta serviços e consultorias relativas a Segurança da Informação.

maliciosas seja no computador, ou sistema de informação.

Figura 2: Principais falhas de segurança e seus incidentes

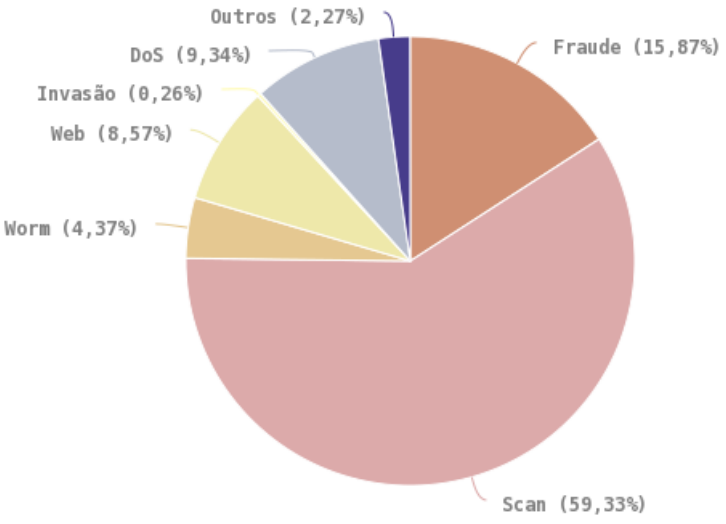


Fonte: (ABCTEC, 2017).

Nota-se através do gráfico que do ano de 1999 a 2015 houve um aumento perceptível no total de incidentes Reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.Br) por ano.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) disponibiliza estatísticas, tais quais: Tipos de ataques (percentual)/ Incidentes Reportados ao CERT.br de Janeiro a Dezembro de 2016, como mostra a Figura 3:

Figura 3: Incidentes reportados ao CERT.br de janeiro a dezembro de 2016



Fonte: (CERT-BR, 2016).

Tem-se a seguinte legenda do gráfico:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

- **dos** (DoS - *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

É importante destacar que não se deve confundir scan com scam. Scams são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Nota-se que a maior percentual se refere a Scan, seguido de Fraude e DoS o que reafirma o aumento e grande expressão dos crimes patrimoniais no Brasil.

3.4 A Criminalidade Cibernética

Em se tratando da criminalidade cibernética ressalte-se que, no ano de 2012 fora sancionada uma Lei que trata do caso em tela, a chamada "Lei Carolina Dieckmann" como ficou conhecida a Lei Brasileira nº 12.737/2012. Este dispositivo legal foi sancionado em 3 de dezembro de 2012, pela Presidente Dilma Rousseff, a qual promoveu, entretanto, algumas alterações no Código Penal Brasileiro, tipificando os chamados "delitos ou crimes

informáticos". A lei acresceu os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal brasileiro (ALMEIDA et al., 2015 apud FRANCESCO, 2014).

A referida legislação é oriunda do Projeto de Lei nº 2793/2011, apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira (PT-SP), que tramitou em regime de urgência e em tempo recorde no Congresso Nacional, em comparação com outros projetos sobre delitos informáticos que as casas de leis apreciavam (como, por exemplo, o PL 84/1999, a "Lei Azeredo", também transformado em lei ordinária 12.735/2012 em 3 de dezembro de 2012) (VIEIRA; ALVES, 2014).

A nova lei ganhou notoriedade porque, antes mesmo de publicada e sancionada, já havia recebido o nome de "Lei Carolina Dieckmann". Tal apelido se deu em razão da repercussão do caso no qual a atriz teve seu computador invadido e seus arquivos pessoais subtraídos, inclusive com a publicação de fotos íntimas que rapidamente se espalharam pela internet por meio das redes sociais (JÚNIOR, 2013).

A partir da sanção dessa lei, crimes desse tipo poderão ser punidos com multas de valores razoáveis e detenção de seis meses a dois anos. Havendo a divulgação, comercialização ou envio das informações sensíveis obtidas na invasão, como comunicações privadas, segredos industriais e dados sigilosos, a pena pode ser elevada em um a dois terços. Caso o crime seja cometido contra o presidente da República, do Supremo Tribunal Federal (STF), governadores, prefeitos, entre outros, a pena será aumentada de um terço à metade.

Um site de segurança da Tecnologia da Internet (TI Inside Online Segurança), publicou seis dicas de segurança para evitar que os dados da empresa vazem na internet. São elas:

1. **Escolha senhas fortes**: Um dos principais erros dos administradores é escolher senhas fracas, de fácil memorização para as contas da empresa, o que facilita a descoberta por hackers. Por isso, escolha senhas fortes, sem obviedade e que não envolvam menções diretas ao nome da organização ou se relacionem com datas (aniversário, fundação da empresa, etc). Mescle números, letras (entre maiúsculas e minúsculas), caracteres especiais e adquira o hábito de mudá-las periodicamente para atestar a segurança das informações.

2. **Selecionar os acessos**: Quando todos os funcionários tem acesso às informações, a organização fica mais vulnerável. O ideal é que os dados de cada setor fiquem restritos a ele. Por exemplo, se ocorre uma invasão às informações do setor de marketing, isso não afetará o setor financeiro. Também é importante levar em conta funcionários agindo de má fé. Por isso, tenha critérios claros de ordem de confidencialidade e selecione os colaboradores que realmente necessitam saber de

informações sigilosas para suas funções diárias.

3. **Use navegação segura**: Habilite todos os navegadores da empresa para utilizarem apenas a navegação segura, ou seja, para sejam barrados qualquer tipo de conexão que não tenha um certificado de segurança, facilitando a disseminação de vírus.

4. **Deixe os colaboradores logados ao Gmail**: Quando uma pessoa está logada automaticamente essa função se ela for desativada por má fé ou por imprudência.

5. **Mantenha o antivírus atualizado**: O antivírus é uma das principais portas de barragem de vírus e trojans (cavalos de troia) que podem ser responsáveis por invasões e roubo de dados e senhas no computador. O software avisa a cada tentativa de invasão e pode apontar para o setor de TI quais máquinas estão apresentando maior fragilidade. Dessa forma, é possível avaliar quais usuários estão fazendo uma navegação imprudente e instruí-los a mudar seus hábitos na rede.

6. **Criptografe seus periféricos**: Um dos principais casos de vazamentos acontece pela perda de periféricos, como pen drives, smartphones, laptops e HDs externos. Uma das formas mais seguras de evitar que outra pessoa tenha acesso às informações nesses dispositivos é o uso da criptografia. Estimule também a realização de backup na nuvem, para que os documentos estejam disponíveis em outro local, sem gerar prejuízos ao trabalho já realizado.

4 CONSIDERAÇÕES FINAIS

Conclui-se que proporcionalmente aos benefícios que surgiram com a internet e ao avanço tecnológico vieram também, condutas ilícitas praticadas por agentes especializados nesse campo. Tais comportamentos são conhecidos de diversas formas, tais como crimes virtuais, crimes cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude informática, crimes transnacionais, dentre outros.

Nesse âmbito, temos a figura do criminoso informático, que possui inteligência, conhecimento de sistemas de informações e usos de meios informatizados com o fim de atingir bens jurídicos alheios, fazendo-se valer de um novo universo de possibilidades de atuação criminosa.

Sabe-se que o Direito Penal encontra muitas dificuldades de adaptação dentro deste contexto. É importante destacar que o Direito em si não consegue acompanhar o frenético avanço que as novas tecnologias e a internet estão proporcionando, e é no ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, também conhecida como criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade e oportunidade de anonimato e da ausência de regras na rede mundial de computadores.

Pode-se afirmar que o ciberespaço é um lugar imaginário, que só temos acesso pelo computador e que os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso são definidos por crimes virtuais.

É incontestável o fato de que o progresso do comércio eletrônico suspira e requer a exigência de estudos e técnicas de combate às fraudes perpetradas no meio virtual. Embora se tenha avançado muito no que concerne a formas de prevenção e detecção dos delitos através da Internet, há uma infinidade de assuntos para serem debatidos e desenvolvidos no setor em voga, tanto por comercialistas quanto por criminalistas.

Nesse mundo de possibilidades ilimitadas, de valores esquecidos e consumo imprudente, a segurança é essencial e, mesmo que seja impraticável chegar a eliminar um dia todos os tipos de infrações, deve-se estar preparado agora para combater de forma veemente tudo que for nocivo ao bem-estar social de uma nação onde o acesso e a utilização da informação são fundamentais.

Sendo assim, todas as ações previstas não são suficientes para coibir as práticas do infrator cibernético. Há a necessidade de regulamentação da internet, o que está sendo discutido pela sociedade atualmente, através do chamado Marco Civil da Internet.

No que tange à conduta transnacional dos infratores cibernéticos, os mesmos

utilizam-se de tecnologia de ponta para encobrirem aspectos relacionados à materialidade dos delitos. Assim, eles se mantêm no anonimato de forma fácil, sendo indispensável uma colaboração internacional, proposta, inclusive, na Convenção de Budapeste, não ratificada pelo Brasil, a qual prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no meio digital através da cooperação internacional.

REFERÊNCIAS

ABCTEC. **O cenário do aumento de incidentes e crimes online no Brasil**. 2017. Acesso em 14/02/2018. Disponível em: <http://www.abctec.com.br/o-cenario-do-aumento-de-incidentes-e-crimes-online-no-brasil>.

ALMEIDA, J. de J. et al. Crimes cibernéticos. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT**, v. 2, n. 3, p. 215–236, 2015.

CASTRO, C. R. A. Crimes de informática e seus aspectos processuais, rev. **Amp. E Atual., Rio De Janeiro, Editora Lumen Juris**, 2003.

CERT-BR. Estatísticas dos incidentes reportados ao cert. br. 2016. Acesso em 12/02/18.

CHAVES, V. H. C. A revolução cibernética: a nova cultura. Universidade Federal de Juiz de Fora, 2015.

COLARES, R. G. Cybercrimes: os crimes na era da informática. **Jus Navigandi, Teresina, ano 6**, 2002.

DESTAK. **Três jovens são presos por suspeita de roubar R$ 400 milhões em 18 meses**. 2018. Acesso em 14/02/2018. Disponível em: <https://www.destakjornal.com.br/cidades/sao-paulo/detalhe/trio-e-preso-por-suspeita-de-roubar-r-400-milhoes-em-18-meses>.

EGO. **Caso de Viviane Araújo vai parar em delegacia de crimes virtuais**. 2014. Acesso em 14/02/2018. Disponível em: <http://ego.globo.com/famosos/noticia/2014/09/caso-de-viviane-araujo-vai-parar-em-delegacia-de-crimes-virtuais.html>.

FANTÁSTICO. **Estupro virtual, em que vítimas são ameaçadas com divulgaçãão de imagens íntimas, cresce**. 2018. Acesso em 14/02/2018. Disponível em: <https://g1.globo.com/fantastico/noticia/2018/12/02/estupro-virtual-em-que-vitimas-sao-ameacadas-com-divulgacao-de-imagens-intimas-cresce.ghtml>.

FERREIRA, I. S. A criminalidade informática, 2ª edição. **São Paulo: Quartier Latin**, 2005.

FRANCESCO, W. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann"**. 2014. Acesso em 14/02/2018. Disponível em: <http://wagnerfrancesco.jusbrasil.com.br/artigos/152372896/o-que-voce-precisa-sabersobrealei127372012conhecidacomoleicarolinadieckmann?utm_campaign=newsletterdaily_20141120_336&utm_medium=email&utm_source=newsletter>.

G1. **Brasil tem a terceira maior taxa de roubos da América Latina, diz Pnud**. 2013. Acesso em 14/02/2018. Disponível em: <http://glo.bo/1dmh48J>.

JR, E. B. C.; AZEVEDO, R. F. L. **Informática aplicada às áreas de contabilidade, administração e economía .** [S.l.]: Editora Atlas SA, 2000.

JÚNIOR, E. Q. d. O. **A nova lei Carolina Dieckmann**. 2013. Acesso em 04/01/2018. Disponível em: <https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>.

LFG. **Crimes contra o patrimônio**. 2017. Acesso em 14/02/2018. Disponível em: <https://www.lfg.com.br/conteudos/artigos/geral/crimes-contra-o-patrimonio>.

LUZ, R. C. d. **Crimes contra o Patrimônio**. Brasília - DF: Conteúdo Jurídico, 2017. Acesso em 20/11/2018. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.589253>.

MANZANO, A. L. N.; IZABEL, N. M. Informática básica. 7ª edição. **São Paulo–Editora Érica**, 2007.

MARCONDES, J. S. **Crimes contra o patrimônio**. 2017. Acesso em 14/02/2018. Disponível em: <https://www.gestaodesegurancaprivada.com.br/crimes-contra-o-patrimonio>.

MARÇULA, M.; FILHO, P. A. B. **Informática: conceitos e aplicações**. [S.l.: s.n.], 2005.

PAGNAN, R.; MARIANI, D. **Crimes contra o patrimônio fazem uma vítima em SP a cada 30 segundos**. 2017. Acesso em 14/02/2018. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2017/08/1909472-crimes-contra-o-patrimonio-fazem-uma-vitima-em-sp-a-cada-30-segundos.shtml>.

PERRIN, S. O cibercrime. **http://vecam. org/article660. html**, v. 7, p. 12, 2006. Acesso em 17/01/2017.

SCHMIDT, G. Crimes cibernéticos. **Jus Brasil**, 2014.

SILVA, R. d. C. L. d. Direito penal e sistema informático. **São Paulo: Revista dos Tribunais**, p. 17–19, 2003.

SOUZA, L. A. de M. A dificuldade da repressão aos crimes virtuais. **Intertem@ s ISSN 1677-1281**, v. 30, n. 30, 2015.

STALLINGS, W.; MIDORIKAWA, E. T. **Arquitetura e organização de computadores: projeto para o desempenho**. [S.l.]: Prentice Hall, 2002.

TANEMBAUM, A. S. Redes de computadores, 4ª edição. **Amsterdam: Vrije Universiteit**, 2003.

TANENBAUM, A. S. **Organização Estruturada de Computadores, 5ª Edição**. [S.l.]: Prentice Hall, 2007.

VIEIRA, A. P.; ALVES, J. C. R. **O direito à privacidade frente aos avanços tecnológicos na sociedade da informação**. 2014. Acesso em 03/01/2018. Disponível em: <http://jus.com.br/artigos/27972/o-direito-a-privacidade-frente-aos-avancos-tecnologicos--na-sociedade-da-informacao/2\#ixzz3K70lVeRz>.

ANEXO A – NOTÍCIAS SOBRE CRIMES CIBERNÉTICOS FAMOSOS

- **Notícia 1**

Três jovens são presos por suspeita de roubar 400 milhões em 18 meses

A polícia desbaratinou ontem 10 de outubro de 2018 uma quadrilha especializada em roubo cibernético que, em 18 meses, conseguiu desviar R$ 400 milhões de contas bancária no país.

Um jovem de 23 anos, suspeito de liderar o grupo, foi preso durante a tarde. Em sua casa foram apreendidos carros de luxo que, juntos, estão avaliados em cerca de R$ 20 milhões. Entre eles estavam Ferraris, Lamborghinis, Porsches, Maseratis e Audis.

Os roubos eram todos feitos via internet. O trio desviava dinheiro de contas bancárias para contas fantasmas. A investigação aponta que foram criadas cinco empresas de fachada para movimentar o dinheiro roubado.

Durante a operação, policiais encontraram joias, duas coroas de ouro e malas de dinheiro. Os três integrantes da quadrilha tiveram prisão provisória decretada. Um deles foi encontrado em um condomínio de alto padrão em Santana de Parnaíba.

Outro foi preso em Francisco Morato enquanto o terceiro integrante foi detido em São Vicente, no litoral paulista. A polícia afirma que ainda não se sabe quantas pessoas foram roubadas, mas que todos os bens apreendidos já foram bloqueados pela Justiça e serão usados para reparar o prejuízo (DESTAK, 2018).

- **Notícia 2**

Estupro virtual, em que vítimas são ameaçadas com divulgação de imagens íntimas, cresce

Começa com uma solicitação de amizade, que logo vira paquera. A vítima envia a primeira foto íntima, o primeiro nude, morde a isca. O suposto namorado passa a chantageá-la, ameaçando compartilhar a foto.

Este caso aconteceu com uma adolescente em Brasília, que ficou refém de um homem que usava perfil falso no Facebook. Ele passou a pedir diariamente fotos e vídeos dela em situações humilhantes.

Segundo site de ajuda a vítimas de crimes de internet, 332 pessoas procuraram ajuda este ano por causa de compartilhamento não-consensual de imagens íntimas: 252 mulheres e 80 homens. Esta semana, no rio, foram presos três suspeitos de estupro virtual (FANTÁSTICO, 2018).

- **Notícia 03**

Caso de Viviane Araújo vai parar em delegacia de crimes virtuais

Atriz teve seu nome envolvido em um vídeo de sexo que circula na internet. Advogada disse ao EGO que vai fazer um registro nesta quinta-feira, 25/09/2014. Após ter seu nome envolvido em um vídeo de sexo que circula na internet, Viviane Araújo está tomando medidas judiciais para esclarecer o caso. Segundo informação da advogada da atriz de "Império", Regina Notini, na próxima quinta-feira, 25, será feito um registro do caso na Delegacia de Repressão aos Crimes de Informática. "Eu recebi esse vídeo pelo meu celular e mostrei a Viviane. O registro tem que ser feito para que a polícia descubra quem publicou tais imagens. Ainda não fomos à delegacia porque Viviane está gravando muito", contou a advogada por telefone nesta terça-feira, 23.

Em conversa com o EGO, a assessoria de imprensa da atriz comentou o seu estado emocional: "Viviane ainda está muito abalada". De acordo com a atriz, além de achar absurda a associação com seu nome, na data que aparece nas imagens ela estava em compromisso com sua escola de samba, o Salgueiro, voltando de um ensaio com amigos.

O vídeo, que tem quase dois minutos de duração, mostra um carro preto parado em uma rua deserta, supostamente às 5h17 de 14 de setembro deste ano. Na sequência, um homem abre a porta, desce do carro, abaixa a calça e, então, a mulher aparece nua e de costas. 'As pessoas não chutam cachorro morto' "Fico me perguntando até que ponto a crueldade do ser humano vai. O que fizeram hoje comigo foi uma crueldade. Colocaram um vídeo como se fosse eu que estivesse fazendo sexo na rua com uma pessoa qualquer. Estou aqui para dizer que não era eu, e tenho como provar que não era eu. Nesse dia estava voltando do Salgueiro com amigos, dentro de uma van. A gente parou para lanchar, e eu tenho como provar tudo isso. E é sempre assim. As pessoas não chutam cachorro morto. Mas Deus está sempre do meu lado", disse Viviane bastante abalada (EGO, 2014).

AUTORIZAÇÃO

Autorizo a reprodução e/ou divulgação total ou parcial do presente trabalho, por qualquer meio convencional ou eletrônico, desde que citada a fonte.

Diamantina, ____ / ____ / _____.

Tamires Aylana de Medeiros Santos

tataaylana@hotmail.com

Universidade Federal dos Vales do Jequitinhonha e Mucuri

Rod. MGT 367, 5000 - Alto da Jacuba, Diamantina - MG, 39100-000.