NATÁLIA LUCAS DO NASCIMENTO

CRIMES CIBERNÉTICOS

Assis
2016

NATÁLIA LUCAS DO NASCIMENTO

CRIMES CIBERNÉTICOS

Projeto de pesquisa apresentado ao Curso de Processamento de Dados do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientanda: Natália Lucas do Nascimento
Orientadora: Márcia Valéria Seródio Carbone

Assis
2016

FICHA CATALOGRÁFICA

Nascimento, Natália Lucas
Crimes Cibernéticos / Natália Lucas do Nascimento. Fundação Educacional do Município de Assis – FEMA – Assis, 2016.
34 folhas

Orientador: Márcia Valéria Seródio Carbone.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis

1. Crime Cibernético 2. Internet 3. Evolução Legislativa

CDD: 340
Biblioteca da FEMA

CRIMES CIBERNÉTICOS

NATÁLIA LUCAS DO NASCIMENTO

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

Orientador: Márcia Valéria Seródio Carbone

Analisador: Maria Angélica Lacerda Marin

Assis
2016

DEDICATÓRIA

Dedico este trabalho a minha família e ao meu noivo, por todo amor dedicado a mim. A Deus por todas as bênçãos alcançadas.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, pela vida, fazendo-me sempre capaz para alcançar meus objetivos e me manter firme para conclusão de mais esta etapa.

Agradecimento especial a minha orientadora Márcia Valéria Seródio Carbone, por toda compreensão, incentivo, didática e paciência para comigo.

Aos meus pais Anésio José do Nascimento e Hiuza Aparecida Lucas do Nascimento, que sempre foram meus alicerces e nunca mediram esforços para me apoiar na realização do curso e de todos meus sonhos.

Ao meu noivo Rodrigo Moreira de Lacerda, futura família, que soube ser paciente, nunca me deixou desistir e faz dos meus sonhos, os dele.

Ao meu filho (a) amado (a), que ainda dentro do meu ventre, me faz cada dia mais forte, sendo o motivo do meu empenho por um mundo mais justo e melhor.

Aos meus amigos que fizeram parte na minha formação na graduação.

Enfim, agradeço a todos que contribuíram direta ou indiretamente para a realização desta monografia. Obrigado por tudo!

Tudo está fluindo. O homem está em permanente reconstrução; por isto é livre: liberdade é o direito de transformar-se.

Lauro de Oliveira Lima

RESUMO

O objetivo do presente trabalho centra-se no estudo da prática dos crimes cibernéticos, o impacto social causado e as soluções encontradas pelo nosso governo para prevenir e combater a prática dos respectivos crimes. Para isso, percorre um breve histórico do surgimento e desenvolvimento da internet a nível mundial. Posteriormente, expõe a evolução histórica e legislativa dos crimes cibernéticos, com ênfase no desenvolvimento da legislação brasileira. Por fim, analisa e discute as diversas denominações que definem os crimes virtuais, indicando os principais programas que servem de ferramentas para a prática do ilícito, bem como os seus principais autores dos referidos crimes.

Palavras-chave: 1. Crime Cibernético 2.Internet 3.Evolução Legislativa.

ABSTRACT

The aim of this work focuses on the practice of the study of cybercrimes, caused social impact and the solutions found by our government to prevent and combat the practice of their crimes. For this, runs through a brief history of the emergence and development of the Internet worldwide. Later, it exposes the historical and legislative evolution of cybercrime , with emphasis on the development of Brazilian legislation . Finally, it analyzes and discusses the various denominations that define cybercrimes, indicating the main programs that serve as tools for the practice of illegal and its main authors of such crimes.

Key words: 1.Cybercrime 2.Internet 3.Legislative Developments.

SUMÁRIO

INTRODUÇÃO

O presente trabalho pretende discutir e analisar as questões relativas à prática dos crimes cibernéticos, o impacto social causado e as soluções encontradas pelo nosso governo para prevenir e combater a prática dos respectivos crimes.

Assim, inicialmente, o primeiro capítulo expõe um breve histórico do surgimento e desenvolvimento da internet, que atualmente transformou-se em uma importante ferramenta de compartilhamento de informações pessoais e comerciais, bem como em um grande espaço para a prática de atos ilícitos.

No segundo capítulo, passa-se a analisar toda a evolução histórica e legislativa dos crimes cibernéticos, com ênfase nas legislações brasileiras, principalmente na Lei n.º 12.695/2014 (Marco Civil da Internet) e a Lei n.º 12.737/2012 (Lei Carolina Dieckmann).

Já no terceiro capítulo, discute e analisa as diversas denominações dos crimes praticados no âmbito virtual, com as suas devidas classificações, expondo, ainda, sobre os diversos crimes cibernéticos, indicando os seus principais autores e as dificuldades encontradas para puni-los.

Por fim, o quarto e último capítulo, expõe de forma analítica os principais assuntos do trabalho, apontando a evolução legislativa ao combate aos crimes cibernéticos, principalmente no Brasil, contudo, indica a necessidade de regulamentar leis específicas para garantir maior eficácia ao combate dos referidos crimes.

1. HISTÓRIA DA INTERNET

A internet, também conhecida como “rede mundial de computadores”, surgiu durante a guerra fria, devido a uma disputa acirrada entre os Estados Unidos da América e a União Soviética, onde os respectivos países compreendiam a eficácia e a necessidade dos meios de comunicação para garantir vantagens e até mesmo a vitória.

Os Estados Unidos, por sua vez, temiam um ataque nuclear russo as suas bases militares, o qual poderia comprometer todas as suas informações, tornando-lhe vulnerável aos seus inimigos.

Portanto, idealizou uma rede de troca e compartilhamento de informações que se descentraliza. Assim, foi criado pela empresa ARPA a rede ARPANET – Advanced Research Projects Agency.

Nota-se, que inicialmente a internet surgiu com a única e exclusiva finalidade de proteger os computadores e informações do Governo Norte Americano. Além do mais, durante determinado tempo à utilização e exploração da internet eram restritas as áreas militares e universitárias, sendo que somente no final da década de 70 e início da década de 80, o sistema passou a ser utilizado para o comércio, devido o surgimento da Rede Minitel na França.

No Brasil, as primeiras redes surgiram em 1988, devido à ligação entre algumas universidades do Brasil com instituições nos Estados Unidos, sendo que com o passar dos anos foi se aprimorando, bem como disponibilizando para o público em geral.

O Ministério da Ciência e Tecnologia do Brasil, através da sua cartilha, define a Internet como um

> sistema de rede de computadores – uma rede de redes – que pode ser utilizado por qualquer pessoa em qualquer parte do mundo, onde haja um ponto de acesso, e que oferece um amplo leque de serviços básicos, tais como correio eletrônico, acesso livre ou autorizado a informações em diversos formatos digitais e transferência de arquivos.

Doravante, ainda na década de 80, foi estabelecido o padrão IP/TCP – Protocolo de internet e Protocolo de Controle de Transmissão, permitindo que o tráfego de

informações fosse percorrido de uma rede para a outra, proporcionando uma troca de mensagens entre todas as redes conectadas pelo endereço de IP na internet.

Já em 1990, o Departamento de Defesa dos Estados Unidos da América, substituiu a rede ARPANET pela rede NSF (Network File System), popularmente conhecida como “internet”, cuja finalidade é o acesso remoto transparente a arquivos/diretórios no servidor, sendo que aparentemente demonstra que o usuário está acessando localmente.

Ademais, para viabilizar a expansão do acesso a internet, foi criado em 1993 pela empresa CERN – Organização Europeia para a investigação Nuclear, o sistema WWW - Word Wide Web, que é um sistema de documentos em hipermídia que são associados e executados na internet, cuja consulta é realizada através do chamado “navegador”.

Portanto, é inevitável afirmar que a cada dia cresce a parcela da população mundial com acesso à internet, na mesma proporção da evolução tecnológica deste sistema, pois o mesmo possibilita a distribuição rápida das informações, facilitando o relacionamento entre as pessoas, sejam elas físicas ou jurídicas, com a finalidade pessoal ou comercial.

1.1 A UTILIZAÇÃO DA INTERNET PARA A PRÁTICA DE CRIMES

Notavelmente a internet apresenta inúmeras vantagens e benefícios para as pessoas, vez que reduziu as distâncias entre as mesmas, possibilitando a realização de relações sociais e comerciais entre as pessoas e nações que estão conectadas a rede, o que, de fato, possibilitou um imenso crescimento econômico dos países que estão conectados a internet.

Isto porque, diariamente convivemos com o comércio e relações sociais virtuais, pois realizamos operações bancárias, consultamos e-mail, notícias e pesquisas, entramos em salas de bate – papo, tudo através da internet.

Nota-se, que a utilização da internet está ligada a inúmeras atividades do nosso dia-a-dia, o que, nos faz reconhecer que a mesma está modificando as nossas relações sociais, pessoais, profissionais e financeiras, sendo que, de igual forma, está criando

diversas condutas danosas a nossa sociedade, ou seja, a conduta criminosa está se aperfeiçoando na mesma proporção do desenvolvimento da internet.

Isto porque, devido à facilidade de comunicação das pessoais e do desenvolvimento das tecnologias, torna-se os crimes praticados com uso de computadores ou via internet mais danosos do que a décadas atrás, vez que dificilmente é possível controlar e até mesmo identificar a sua origem, pois não existem fronteiras entre os chamado “cyberspace”, ou seja, “ciberespaço”.

O ciberespaço é um espaço virtual abrangido pela internet que reduziu fronteiras e aproximaram as pessoas, formando uma nova dimensão espacial que permite a todos aqueles conectados a rede um contato imediato com qualquer pessoa localizado em qualquer lugar do mundo em segundos.

Deste modo, pode-se perceber que da mesma forma que a internet traz benefícios imensuráveis a população mundial, também proporciona práticas ilícitas que podem causar danos às pessoas conectadas a rede.

Portanto, um dos principais desafios atualmente é conseguir monitorar e reprimir a prática de condutas ilícitas via internet, regulamentando leis eficazes ao combate a crimes cometidos sob a utilização da rede mundial de computadores.

Na realidade, o objetivo do presente trabalho é refletir sobre a prática dos crimes de informática, as suas consequências na atual sociedade, bem como as soluções que nosso governo tem apresentado para o tema.

2. DA EVOLUÇÃO HISTÓRICA E LEGISLATIVA DOS CRIMES CIBERNÉTICOS

Os primeiros casos de crimes virtuais ocorreram na década de 1960, onde os infratores manipulavam os dados contidos nos computadores, praticando atos de sabotagem, espionagem e abuso ilegal de sistema de computadores, contudo, era muito difícil de detectar a prática de tal ato devido às condições técnica daquela época.

Todavia, a partir de 1980, houve uma alteração radical sobre o tema, vez que foram identificadas e divulgadas diversas ações criminosas com a utilização de meios virtuais, tais como pirataria de programas, manipulação de valores nos caixas eletrônicos, abuso de telecomunicação, entre outros.

Assim, com a intensa prática dos crimes de informática durante o referido período, foram surgindo as primeiras legislações que regulamentavam a prática dos respectivos atos ilícitos.

Por mais uma vez, os Estados Unidos da América foram pioneiros no assunto, quando em 1984 editaram a legislação “Crime Control Act” e logo em seguida o “Computer Fraud and Abuse Act, em 1986.

A Alemanha, em 1986, editou a Lei “Computer Kriminalitat”, seguida da Franca que em 1988 editou a Lei Godfrain. Posteriormente, em 1995 a Espanha incluiu crimes de informática na reforma do seu Código Penal.

Em 23/11/2001, o Conselho da Europa (Council of Europe), elaborou a Convenção Europeia sobre Crimes Cibernéticos, objetivando uniformizar a legislação europeia quanto à politica criminal dos crimes cibernéticos, contudo, esta convenção será devidamente discutida em um tópico específico.

No Brasil, inicialmente o tema foi tratado como uma questão de direito penal econômico, vez que no dia 18/12/1987 foi editada a Lei n.º 7.646/87, cuja finalidade é a proteção à propriedade intelectual sobre programas de computador e sua comercialização no país.

Mais tarde, foi editada a Lei n.º 8.137/1990, o qual define crimes praticados contra a ordem tributária. Ademais, somente com edição da Lei n.º 9.883/2000, o legislador

passou a abranger a regulamentação de outros delitos relacionados à internet que não sejam de ordem econômica. A respectiva legislação tem a finalidade de proteger os dados e os sistemas de informação, punindo principalmente os crimes próprios de funcionários públicos que violem o sistema de informação da Administração Pública.

Por fim, recentemente houve a edição da Lei n.º 12.695/2014, popularmente conhecida como “Marco Civil da Internet”, que regulamenta a utilização da internet estabelecendo princípios e normas que asseguram uma maior proteção aos usuários da internet, contudo, a importância desta lei será amplamente discutida a seguir.

2.1 DA LEI N.º 12.695/2014 – MARCO CIVIL DA INTERNET

O “Marco Civil da Internet” foi criado através de uma incorporação de vários projetos similares, que ganharam força principalmente pelas descobertas de espionagem do Governo Norte Americano contra o Brasil e outros países.

Assim, no dia 23/04/2014 a Lei n.º 12.695/2014 foi sancionada pela então presidente Dilma Rousseff, o qual estabelece princípios, garantias, deveres e direitos aos usuários da internet.

O capítulo I, do referido dispositivo legal, dispõe sobre conceitos, princípios, direitos e deveres para a utilização da internet a nível nacional, bem como estipula diretrizes para a atuação do poder público em relação à matéria.

No capítulo II, dispõe sobre direitos e garantias dos usuários, estabelecendo proteção à intimidade e a vida privada dos usuários, além de assegura-los o direito de informações claras e precisas quanto às políticas de uso dos sites, provedores e redes sociais.

O capítulo III estabelece provisão de conexão e de aplicações de internet, onde define inúmeras normas. A neutralidade da rede é uma das diretrizes que foram estabelecidas neste capítulo, sendo que esta é de fundamental importância, pois institui ao responsável pela transmissão, comutação ou roteamento da obrigação de

tratar de forma isonômica qualquer pacote de dados, sem distinção pela sua origem, destino, conteúdo, serviço, terminal ou aplicação.

Além do mais, nos casos acima mencionados é vedado o bloqueio, monitoramento, filtro ou análise do conteúdo dos pacotes de dados, sob pena reparação dos danos causados.

Ademais, os registros dos dados pessoais e das comunicações privadas possuem uma proteção especial, vez que determinam ao provedor atender a preservação da intimidade, da vida priva, da hora e da imagem de todas as partes diretamente ou indiretamente envolvidas, sob pena de aplicação de sanções cíveis, criminais e administrativas, de acordo com a gravidade da infração.

Ainda, institui a responsabilidade por danos causados por terceiros, estabelecendo que o provedor não será responsabilizado civilmente pelos danos decorrentes de conteúdo de terceiros, salvo no caso de descumprimento de ordem judicial, o qual o provedor não tomou as devidas providencias dentro do prazo legal.

Por outro lado, o capítulo IV, aborda diretrizes para a atuação dos entes públicos no desenvolvimento da internet no Brasil.

Por fim, o capítulo V, dispõe sobre disposições finais estabelecendo a liberdade de escolha do usuário na utilização de programa de computador, além de estimular a defesa dos seus interesses e direitos estabelecidos na presente Lei no âmbito administrativo e judicial.

2.2 DA LEI N.º 12.737/2012 – LEI CAROLINA DIECKMANN

A Lei n.º 12.737/2012, popularmente conhecida como “Lei Carolina Dieckmann”, foi sancionada no dia 03/12/2012 pela então presidente Dilma Rousseff, o qual alterou alguns artigos do Código Penal Brasileiro, tipificando delitos cometidos através dos meios virtuais.

Destaca-se, que a proposta da referida lei tramitou no Congresso Nacional através do Projeto de Lei n.º 2793/2011, sendo que a principal referência era a situação que

a atriz Carolina Dieckmann passou em maio de 2011, quando supostamente teve copiado do seu computador pessoal, fotos íntimas que foram divulgadas na internet.

Portanto, é por tais motivos que a Lei n.º 12.737/2012 é popularmente conhecida como “Lei Carolina Dieckmann”.

Doravante, conforme já mencionado, a referida lei acrescentou e modificou alguns artigos do Código Penal Brasileiro.

O Artigo 154-A, por exemplo, tipifica como ilícita a conduta de um individuo que invade um computador alheio, conectado a rede ou não, com a finalidade de obter, adulterar ou destruir dados sem a autorização expressa ou tácita do titular do dispositivo violado, aplicando uma pena de 3 (três) meses a 1 (um) ano de detenção, e multa, podendo, ainda, a pena ser aumentada de um sexto a um terço quando a invasão resultar em prejuízos financeiros.

Por outro lado, caso a invasão tenha resultado na obtenção imprópria do conteúdo de comunicações privadas, segredos comerciais e informações sigilosas, a pena é de reclusão de 6 (seis) meses a 2 (dois) anos, e multa, podendo ainda ser aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro.

Ademais, a pena é aumentada de um terço à metade se o crime for praticado contra o Presidente da República, da Câmera dos Deputados, do Senado Federal, da Assembleia Legislativa do Estado, da Câmara Legislativa Federal e Municipal, dos Governadores, dos Prefeitos, do Presidente do Supremo Tribunal Federal e dos dirigentes máximos da administração pública direta e indireta, sejam de competência federal, estadual, municipal ou distrital.

Por fim, a lei regulamenta sobre interrupção ou perturbação de serviços informáticos, além de falsificação de documento particular e de cartão de crédito utilizando a internet.

2.3 DA CONVENÇÃO EUROPEIA SOBRE CRIMES CIBERNÉTICOS – CONVENÇÃO DE BUDAPESTE.

A Convenção Europeia sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, elaborada em 23/11/2001 pelo Conselho da Europa (Council of Europe), órgão intergovernamental que engloba 45 Estados membros, inclusive os membros da União Europeia, é o primeiro tratado internacional sobre crimes cometidos através de sistemas de computadores, cujo principal objetivo é uniformizar a legislação europeia quanto a política criminal dos crimes cibernéticos.

Ademais, a referida convenção está dividida em quatro capítulos, os quais integram cinco títulos.

O primeiro capítulo trata das terminologias, definindo termos como “sistema de computador” (computer system), provedor de serviços (servisse provedor), entre outros, objetivando uniformizar as definições.

Já nos capítulos seguintes, estão previstas medidas para serem tomadas no âmbito das legislações nacionais, estabelecendo leis penais, normas processuais e de investigação, além de criminalizar certas condutas.

O Título I da referida Convenção, determina quais infrações devem ser definidas a nível nacional aos países signatários contra a confidencialidade integridade e disponibilidade de sistemas e dados informáticos.

O Titulo II, dispõe sobre infrações relacionadas a computadores, tais como a falsidade e burla informática, os quais correspondem respectivamente a introdução, modificação e eliminação de dados informáticos.

No Titulo III, institui algumas infrações, porém, em especial a regulamentação da pornografia infantil. Por outro lado, o Título IV, aborda infrações relacionadas à violação a direito de autor e direitos conexos.

Por fim, no Título V, faz referência as formas de responsabilidade e sanção, abordando temas de ordem processual como, por exemplo, a busca e a apreensão de dados armazenados em sistemas informáticos, além de dispor sobre a obrigação do fornecedor de serviços registrar todas as informações, bem como transmiti-las para as autoridades competentes quando solicitadas.

Ressalta-se, ainda, que a Convenção dispõe que quando existir pluralidade de partes reivindicando a competência para processar e julgar a prática de uma suposta infração prevista na convenção, devem todas as partes envolvidas reunir-se para consentir na jurisdição mais apropriada.

Como se vê, a Convenção de Budapeste é um importante instrumento de combate aos crimes cibernéticos, pois além de unir os países signatários para regulamentar um problema em comum, procura uniformizar as normas de combate à prática destes crimes.

O Brasil, por sua vez, ainda não é um país signatário da Convenção de Budapeste, contudo, já regulamentou algumas normas com a mesma finalidade, ou seja, de regulamentar o uso da internet pelos seus usuários e criminalizar condutas ilícitas praticadas via internet.

3. DOS CRIMES CIBERNÉTICOS

As atividades ilícitas praticadas com a utilização de computadores via internet ainda não possuem uma denominação definitiva. Assim, são chamadas de cibercrimes, crimes informáricos, crimes cibernéticos, entre outros.

Todavia, todas essas denominações se referem ao mesmo tipo de crime, ou seja, crimes que utilizam-se de um computador ou de internet como instrumento para praticar atos ilícitos.

3.1 DA CLASSIFICAÇÃO DOS CRIMES

Como vimos, o que define o crime de informática é a utilização do computador ou da internet para a prática do ato. Assim, podem ser classificados como crimes cibernéticos puros e impuros.

3.1.1 Crimes Cibernéticos Puros

Os crimes cibernéticos puros ocorrem quando o agente quer atacar o sistema de informática de um terceiro, seja este sistema um software, hardware, sistema e meios de armazenamento de dados.

Segundo Damásio de Jesus:

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

Nota-se, que esta categoria de crime caracteriza-se quando um individuo, principalmente o hacker e o cracker, utiliza-se de um computador e/ou internet para

invadir a máquina de um terceiro, sendo que o crime se consome no próprio meio virtual, não produzindo efeitos fora deste ambiente.

3.1.2 Crimes Cibernéticos Impuros

Os crimes cibernéticos impuros ocorrem quando o agente utiliza-se da internet como meio executório para prática de um crime tipificado em nossa legislação penal, como por exemplo, a divulgação de fotografias pornográficas de crianças e adolescentes, tipificada no Art. 241 do Estatuto da Criança e do Adolescente.

Damásio de Jesus, conceitua o referido crime da seguinte forma:

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

Desta forma, os crimes impuros são aqueles em que o agente utiliza-se do computador e da internet como ferramenta meio para produzir um resultado que afeta outros bens tutelados pelo nosso ordenamento jurídico que não sejam relacionados aos meios virtuais.

3.2 RELAÇÃO DE CRIMES CIBERNÉTICOS SEGUNDO A ONU

A ONU – Organização das Nações Unidas, no 8º Congresso sobre Prevenção de Delito e Justiça Penal, realizado em Havana em 1990, elaborou uma relação de crimes relacionados aos meios informáticos. Senão vejamos:

1º - fraudes cometidas através de manipulação de computadores;

2º - falsificações informáticas;

3º - danos ou modificações de programas ou dados computadorizados,

Após uma década, mais precisamente no ano 2000, a ONU relacionou outros tipos de crimes cibernéticos, elaborados no 10º Congresso sobre Prevenção de Delito e Tratamento de Delinquente, realizado em Viena, os quais seguem a baixo:

1º - espionagem industrial para descoberta de segredos comerciais, técnicas e estratégias; sabotagem de sistemas;

2º - sabotagem e vandalismo de dados;

3º - lavagem de dinheiro;

4º - jogos de azar; fraudes, principalmente contra consumidores;

5º - pornografia infantil;

6º - estratagemas, com intuito de buscar sistemas restritos;

7º - averiguação de senhas secretas.

3.3 PROGRAMAS CRIMINOSOS

É cediço que os criminosos utilizam-se do computador e da internet para praticar crimes cibernéticos, e para isso usam predominantemente software (programa de computador) como ferramenta para atingir os seus objetivos, ou seja, de consumar o ato ilícito.

Atualmente, existem diversas nomenclaturas que identificam os softwares criminosos, tais como os cookies; spywares; spammings; hoaxes; sniffer; cavalo de troia; backdoors; vírus e worm.

Os cookies são pequenos pacotes de dados enviados de um website para o navegador do usuário, o qual registra todas as informações das suas atividades. Ocorre que, quando este programa é utilizado por criminosos, podem tem acesso a todas as informações prestadas pelo usuário, inclusive números de cartões de crédito e senhas.

Já spywares é um tipo de programa espião que retira todas as informações do computador do usuário, sem o seu consentimento, e transmite-os para outro usuário de rede desconhecida. Isto ocorre quando o usuário acessa um website que imediatamente introduz o programa espião que é instalado, sendo que, a partir de então, inicia a coleta de informações.

Por outro lado, os spammings, são programas que enviam mensagens eletrônicas, em especial publicitárias, sem ao menos serem solicitadas pelo usuário, os quais sobrecarregam a caixa eletrônica, além de invadir a sua privacidade. Não obstante, este tipo de programa pode introduzir cookies capazes de espionar o usuário, o que, de fato, facilita prática de crimes cibernéticos.

Os hoaxes são muito utilizados na internet, pois enviam e-mails com conteúdos que causam grande comoção social, como por exemplo mensagens de cujo sentimental, dramático ou religioso, sendo que muita das vezes se passam por empresas ou órgãos governamentais, enviando mensagens com a finalidade de causar desinformação acompanhadas de vírus.

O sniffer é um programa espião e um pouco parecido com os spywares, sendo que a sua finalidade é invadir os hardwares dos computadores para coletar informações do usuário.

De igual forma, o cavalo de troia também é um programa espião, o qual se apropria de informações, arquivos e senhas contidos no computador do usuário invadido. O referido programa é instalado quando o usuário abre um arquivo que recebeu que consequentemente possibilita ao invasor controlar o seu computador, podendo copiar e excluir todos os arquivos detectados.

Por outro lado, os backdoors, por sua vez, se assemelham com o cavalo de troia, contudo, são objetos de projetos de programas com defeitos ou falhas de fabricação, que são enviados aos usuários de forma culposa ou dolosa.

Os vírus, que são verdadeiras doenças contagiosas que podem comprometer todos os programas e configurações dos computadores, são demasiadamente transmitidos aos usuários através de e-mails, vídeos, músicas, CDs, dispositivos USB, entre outros. Após a sua instalação, o invasor poderá ter acesso a todas as informações contidas no computador do usuário, além de continuar infectando outras repartições do referido dispositivo eletrônico.

Por fim, o Worm é um programa que se espalha de um sistema para o outro sem a intervenção do usuário infectado, cuja finalidade é exclusivamente eliminar arquivos do computador.

3.4 DA AUTORIA DOS CRIMES CIBERNÉTICOS

Os crimes eletrônicos podem ser praticados por qualquer pessoa, seja esta pessoa física ou jurídica. Todavia, existem predominantemente indivíduos específicos que praticam infrações ou crimes virtuais, os quais são denominados de hacker, cracker, pheakers, cardes e cyberterrorists.

As denominações supramencionadas são do idioma inglês, vez que evidentemente é a linguagem oficial utilizada na internet, o qual identifica diversas ferramentas e serviços oferecidos pela Rede Mundial de Computadores, sendo que, de igual forma, identifica os sujeitos ativos que praticam os crimes cibernéticos.

Pois bem, o termo hacker identifica um individuo que possui habilidade técnica para conhecer e alterar todo e qualquer dispositivo eletrônico, programa e comunicações via internet. Na grande maioria das vezes, os hackers são jovens estudantes que invadem sistemas informáticos alheios, motivados principalmente pela curiosidade, com intuito de satisfazer o seu próprio ego.

Por outro lado, os crakers são indivíduos especialistas em invadir sistemas alheios de forma ilegal e antiética, objetivando causar um dano à vítima, alterando programas e dados e subtraindo informações do computador e da rede.

Os pherakers são indivíduos especialistas em telefonia, que visam exclusivamente fraudar sistemas de telecomunicações utilizando-se de linhas telefônicas convencionais ou de aparelhos celulares clonados para realizar ligações clandestinas, os quais facilitam ataques a sistemas externos, bem como dificultam o seu rastreamento.

Já os cardes são indivíduos que se apropriam de números de cartões de crédito subtraídos de sites de compras pela internet, utilizando programas espiões instalados nos computadores das vítimas.

Por fim, os cyberterroristas são aqueles que desenvolvem vírus de computadores, bem como as chamadas bombas lógicas que causam queda do sistema de grandes provedores, o que, consequentemente, impede o acesso do usuário ao sistema, podendo ainda lhe causar prejuízos econômicos.

3.5 TEMPO E LOCAL DO CRIME

Destaca-se que no âmbito dos crimes informáticos é extremamente difícil indicar o exato momento da prática do ato ilícito, para que seja aplicada a consequente sanção penal.

Isto porque, no meio informático existe uma dissociação temporal, pois é possível programar a execução de um crime informático no tempo, ou seja, o ato ilícito pode ser executado meses após a sua programação, devido o fato de todo computador possuir um relógio interno.

O nosso Código Penal, adotou a teoria da atividade para descrever o momento do crime. Portanto, a prática de um crime ocorre no momento da ação ou omissão, independentemente do momento do resultado.

Todavia, no mundo virtual não existe um espaço físico predeterminado e tão pouco um espaço geograficamente delimitado. Assim, para a constatação da prática de um determinado crime informático é necessário detectar a localização da informação, pois esta será essencial para proporcionar a ideia de território.

Ademais, cumpre esclarecer ainda que o espaço virtual é denominado de “ciberespaço”, que indica o local onde ocorre todo fluxo de informações através das redes de comunicações.

Desta forma, grande parte dos crimes virtuais superam fronteiras territoriais, pois o mundo está conectado à internet.

Isto posto, como não existe legislação processual penal nacional para esta matéria, é necessário a aplicação de alguns princípios do Código Penal Brasileiro, mais precisamente quanto a territorialidade, extraterritorialidade, nacionalidade, defesa e representação.

Com relação à territorialidade, previsto no Art. 5º do Código de Penal Brasileiro, determina que seja aplicado a lei penal brasileira a todos os crimes executados em território nacional, sem prejuízo das normas, convenções e tratados de Direito Internacional.

Já com relação aos demais princípios, os quais estão previstos no Art. 7º do Código Penal Brasileiro, conduz a extraterritorialidade da lei penal nacional, determinando a aplicação da nossa legislação penal para os crimes praticados fora do nosso território nacional.

Neste aspecto, mesmo que o crime tenha ocorrido no exterior, à legislação penal nacional poderá ser aplicada nas seguintes hipóteses. Senão vejamos:

1º - quando o indivíduo for brasileiro;

2º - quando o bem lesionado for brasileiro, seja este objeto ou pessoa;

3º - quando o crime for transnacional, e o Brasil comprometido a reprimir tal conduta criminosa, através de tratados ou convenções;

4º - quando o crime ocorrer no interior de aeronaves ou embarcações brasileiras, mercantis ou de propriedade privada, ainda que em território estrangeiro, caso não tenha sido julgado.

Ressalta-se, que caso seja caracterizado o caso de extraterritorialidade condicionada, deve ser respeitada os requisitos previstos no Art. 7, §§ 2º e 3º do Código Penal Brasileiro.

Já com relação ao lugar do crime, o Código Penal Brasileiro adotou a teoria da ubiquidade, o qual define o local do crime onde ocorreu a ação ou a omissão, no todo ou em parte, bem como onde se produziu o resultado.

Portanto, todo crime informático que tenha ocorrido em todo ou em parte em nosso território nacional poderá ser objeto de aplicação da legislação penal brasileira.

3.6 DA COMPETÊNCIA

Com relação à competência dos crimes informáticos, na grande maioria dos casos, é de responsabilidade da Justiça Federal, tendo em vista o predominante sentido transnacional do crime.

Neste aspecto, o Art. 109 da Constituição Federal de 1988, delimita as hipóteses em que compete a Justiça Federal processar e julgar a prática de determinados crimes, principalmente aqueles cometidos contra a Administração Pública Federal e que ultrapassam as fronteiras nacionais.

Além do mais, os crimes de racismo e de pedofilia praticados via internet, devem ser processados e julgados pela Justiça Federal, por expressa previsão em convenções internacionais de direitos humanos.

Por outro lado, os crimes contra a honra praticados via internet devem ser processados e julgados pela Justiça Estadual.

3.7 DA ESCASSA PREVISÃO LEGAL QUANTO À PRÁTICA DE CONDUTAS ILÍCITAS VIA INTERNET

As condutas ilícitas praticadas via internet causam imensuráveis dificuldades práticas para punir os infratores, vez que ainda existem parcas legislações que tipificam estas condutas, existindo, portanto, inúmeras impunidades pela prática de condutas ilícitas e antiéticas no âmbito virtual.

Destaca-se, que a Lei n.º 12.695/2014, mais conhecida como Marco Civil da Internet, trouxe grandes avanços relacionados ao uso da internet, pois instituiu deveres e direitos aos usuários da internet.

Entretanto, o extraordinário crescimento da criminalidade no âmbito da informática, infelizmente é maior de que a prevenção e evolução legislativa quanto o regulamento da matéria.

Assim, atualmente no Brasil aplica-se a legislação penal vigente, através de enquadramento jurídico, que em sua maioria não regulamentam especificadamente a matéria, tais como crime contra a honra e ameaça, além de furto de valores em

conta bancária, preconceitos e discriminações, e envio de fotografias e vídeos relacionados a criança e o adolescente.

Diante do exposto, é necessário regulamentar especificadamente cada conduta ilícita praticada nos meios virtuais para que seja reduzido o número de lacunas legislativas relacionadas aos crimes virtuais.

3.8 DA PREVENÇÃO

Como vimos, os crimes virtuais podem ser praticados por qualquer pessoa e, principalmente, por especialistas tais como os craques e cyberterrorists.

Portanto, para evitar ser vitima da prática destes crimes, é necessário tomar algumas prevenções para evitar que o dispositivo eletrônico seja invadido, seja este um computador ou celular, ou, se por a caso isto ocorrer, providenciar o resguardo das provas.

Pois bem, é necessário manter o computador protegido com programa de antivírus atualizado. Este programa pode impedir ou pelo menos dificultar a invasão do computador por terceiros, detectando e eliminando qualquer vírus que for localizado.

Ademais, é necessário se policiar a respeito dos sites que pretende visitar, devendo necessariamente analisar se é de confiança.

Por outro lado, quando alguma pessoa for vítima de ofensas praticadas via internet, é necessário preservar todas as provas, haja vista que no ambiente virtual as páginas podem ser modificadas a qualquer momento, o que, de fato, pode acarretar grandes dificuldades nas investigações para punir o infrator.

Assim, quando o crime informático deixar vestígios que se substanciam em ilícitos materiais, deve ser realizada uma perícia para analisar todas as provas e demonstrar a materialidade e autoria do crime.

Deste modo, é necessário tomar todas as providencias possíveis para evitar ser vítima de qualquer crime informático, e caso isso ocorre, deve ser todas as provas preservadas para facilitar as investigações e consequentemente punir os infratores que praticaram o ato ilícito.

4. CONCLUSÃO

Como vimos, a internet é um importante meio de comunicação que cresce a cada dia devido ao grande número de pessoas que utilizam desta ferramenta para compartilhar informações com a finalidade pessoal ou comercial.

Assim, evidentemente que a internet nos proporciona inúmeros benefícios, contudo, da mesma forma, possibilita a prática de atos ilícitos os quais prejudicam de diversas formas os usuários conectados à rede.

A grande maioria dos crimes cibernéticos são praticados com a utilização de softwares criminosos, tais como os cookies; spyware; spammings; hoaxes; sniffer; cavalo de troia; backdoors; vírus e Worm.

Destaca-se, que os referidos crimes podem ser praticados por qualquer pessoa, contudo, evidentemente, existem indivíduos específicos tais como os hackers; craker; pherakers; cardes e cyberterrorists.

Ocorre que, a grande dificuldade é indicar com precisão o tempo e o local do crime cibernético. Isto porque, primeiro, no âmbito virtual não existem espaços físicos predeterminados, segundo, é possível programar a execução do crime no tempo.

Desta forma, é essencial a identificação da localização da informação, pois será a partir desta constatação que proporcionará a ideia de território, para que, consequentemente, seja aplicada a sanção penal competente.

Todavia, atualmente ainda existem parcas legislações que tipificam as condutas criminosas no âmbito virtual, o que, de fato, dificulta a punição dos infratores.

No Brasil, recentemente foi aprovado a Lei n.º 12.695/2014, popularmente conhecida como Marco Civil da Internet, que trouxe inúmeros avanços quanto aos direitos e deveres dos usuários e provedores da internet, porém, infelizmente, por si só ainda não é suficiente ao combate aos crimes cibernéticos que crescem de forma extraordinária.

Portanto, é necessário regulamentar leis específicas para o combate ao crime cibernético, bem como que haja investimentos de proteção na segurança das informações dos dados dos usuários.

REFERÊNCIAS

BARROS, Marco Antônio de/ Garbossa, Daniella D`Arco/ Conte, Christiany Pegorari. **CRIMES INFORMÁTICOS E A PROPOSIÇÃO LEGISLATIVA: CONSIDERAÇÕES PARA UMA REFLEXÃO PRELIMINAR. Revista dos Tribunais** | vol. 865/2007 | p. 399 - 433 | Nov / 2007. Doutrinas Essenciais de Direito Penal | vol. 8 | p. 981 - 1027 | Out / 2010. DTR\2007\931.

BOITEUX, Luciana. **CRIMES INFORMÁTICOS: REFLEXÕES SOBRE POLÍTICA CRIMINAL INSERIDAS NO CONTEXTO INTERNACIONAL ATUAL. Revista Brasileira de Ciências Criminais** | vol. 47/2004 | p. 146 - 187 | Mar - Abr / 2004 Doutrinas Essenciais de Direito Penal | vol. 8 | p. 945 - 979 | Out / 2010 DTR\2004\156.

CASABONA, Carlos María Romeo. **DOS DELITOS INFORMÁTICOS AO CRIME CIBERNÉTICO: UMA APROXIMAÇÃO CONCEITUAL E POLÍTICO-CRIMINAL.** Ciências Penais | vol. 4/2006 | p. 83 - 121 | Jan - Jun / 2006. **Doutrinas Essenciais de Direito Penal Econômico e da Empresa** | vol. 6 | p. 509 - 552 | Jul / 2011. DTR\2006\22.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. Editora: SARAIVA JURIDICO. Ano de Edição: 2010.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. Editora Juarez de Oliveira. Ano 2009.

JUNIOR, Geraldo Frazão de Aquino. **RESPONSABILIDADE CIVIL NA INTERNET. Revista de Direito Constitucional e Internacional** | vol. 86/2014 | p. 451 - 473 | Jan - Mar / 2014. Doutrinas Essenciais de Dano Moral | vol. 1/2015 | p. 451 - 473 | Jul / 2015. DTR\2015\9886.

MATTOS, Alexandre M. **Crimes na Internet.** Editora: Espaço Jurídico. ANO DE EDIÇÃO: 2012.

SILVA, Cássia Lopes da. **A Informação como Bem Jurídico-Penal e o Sistema Informático**. Ciências Penais | vol. 7/2007 | p. 242 - 254 | Jul - Dez / 2007. **Doutrinas Essenciais de Direito Penal Econômico e da Empresa** | vol. 6 | p. 579 - 593 | Jul / 2011. DTR\2007\389.

http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529 (visita em 27/07/2016)

https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o (visita dia 02/08/2016)

https://pt.wikipedia.org/wiki/Internet (visita dia 25/07/2016)

https://pt.wikipedia.org/wiki/Lista_de_pa%C3%ADses_por_n%C3%BAmero_de_usu%C3%A1rios_de_Internet (visita dia 26/07/2016)

http://www.mcti.gov.br/ (visita dia 25/07/2016)

http://www.cnasi.com.br/crimes-ciberneticos-a-vitima-e-voce/ (visita dia 25/07/2016)

https://pt.wikipedia.org/wiki/Crime_inform%C3%A1tico (visita dia 31/07/2016)

http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17 (vista dia 28/08/2016)

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (visita dia 26/07/2016)

https://www.oficinadanet.com.br/post/12558-o-marco-civil-da-internet-foi-aprovado-entenda-o-que-e-e-o-que-muda-na-sua-vida (visita dia 26/07/2016)

https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann (visita dia 27/07/2016)

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm (visita dia 27/07/2016)