CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO
DE PRESIDENTE PRUDENTE

FACULDADE DE DIREITO

A DIFICULDADE DA REPRESSÃO AOS CRIMES VIRTUAIS

Larissa Anne de Moraes Souza

Presidente Prudente/SP
2015

CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO
DE PRESIDENTE PRUDENTE

FACULDADE DE DIREITO

A DIFICULDADE DA REPRESSÃO AOS CRIMES VIRTUAIS

Larissa Anne de Moraes Souza

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação da Prof. Ms. Ana Laura Teixeira Martelli Theodoro.

Presidente Prudente/SP
2015

A DIFICULDADE DA REPRESSÃO AOS CRIMES VIRTUAIS

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

Ana Laura Teixeira Martelli Theodoro

Fernanda de Matos Lima Madrid

Guilherme Prado Bohac de Haro

Presidente Prudente, 28 de Maio de 2015.

Não há melhor maneira de exercitar a imaginação do que estudar direito. Nenhum poeta jamais interpretou a natureza com tanta liberdade quanto um jurista interpreta a verdade.

Jean Giraudox

AGRADECIMENTOS

Primeiramente a Deus, por ter me dado o dom da vida e capacidade, para que eu pudesse chegar nesse momento e concluir mais uma etapa de minha vida.

À minha mãe, Eunice, porque sem ela nada teria sido possível e quem nunca mediu esforços para que eu pudesse vencer não só essa etapa acadêmica, mas todas as grandes fases da minha existência.

À minha orientadora, Dra. Ana Laura Teixeira Martelli Theodoro, por sua sensibilidade que a diferencia como educadora e por sua disposição, paciência, e inspiração no amadurecimento dos meus conhecimentos que me levaram a execução e conclusão desta monografia.

À minha avó, Creuza, que com a sua imensa sabedoria, me aconselhou e contribuiu para que este momento fosse possível.

Ao meu irmão, Marcus, pela amizade e companheirismo de sempre.

A todos os meus amigos por estarem sempre ao meu lado e por sempre me apoiarem em todos os momentos da minha vida.

Enfim, agradeço a todos, que durante esses anos contribuíram não só para o meu crescimento e amadurecimento profissional, mas também, para o meu crescimento pessoal.

RESUMO

O presente trabalho enfoca as dificuldades encontradas na repressão aos crimes virtuais. Leva-se em consideração que com a criação e a evolução da internet e dos meios de utilização desta, a propagação de uma informação ocorre rapidamente, e com o crescente uso dessa tecnologia, o Direito apresenta enormes dificuldades para acompanhar e punir as condutas delitivas ocorridas nesse ambiente. Assim, o início deste relata os acontecimentos históricos que foram relevantes para o surgimento dos crimes cibernéticos, sendo eles a história do computador, o surgimento da internet e o histórico dos crimes de internet. Em seguida um esboço mais aprofundado quanto aos crimes digitais tendo em vista o seu conceito, seus sujeitos ativo e passivo, os bens jurídicos tutelados e as classificações das condutas incriminâveis. E por fim, objetiva-se mostrar os maiores problemas encontrados para que ocorra a identificação e a punição dos autores de crimes virtuais, levando em consideração a carência de uma estrutura adequada no país para que maiores resultados positivos sejam obtidos.

Palavras-chave: Crimes Virtuais. Internet. Computador. Dificuldade de Repressão. Crimes Cibernéticos.

ABSTRACT

The present research focuses the difficulties encountered in repression to cybercrime. It takes into account that with the creation and the evolution of the Internet and means for using this, the spread of information occurs rapidly, and the increasing use of this technology, Law presents enormous difficulties to monitor and punish the criminal behaviors occurred in this environment. Thus, the beginning of this report historical events that were relevant for the emergence of cybercrimes, and then, the history of computer, the emergence of the Internet and the history of internet crimes. Then further outline as to cybercrime in view of its concept, its assets and liabilities subjects, the legally protected interests and classifications of incriminates conducts. Finally, the objective is to show the main problems found to occur identification and the punishment of perpetrators of cybercrimes, taking into account the lack of adequate infrastructure in the country to major positive results are obtained.

Keywords: Cybercrimes. Internet. Computer. Difficulty Repression. Cybercrimes.

LISTA DE ABREVIATURAS E SIGLAS

ARPANET – Advanced Research Projects Agency Network

FBI - Federal Bureau of Investigation, Agência Federal de Investigação

IP – Internet Protocol, Protocolo de Interconexão

NASA – National Aeronautics and Space Administration, Administração Nacional do Espaço e da Aeronáutica

NREN – National Research and Education Network

NSFNET – National Science Foundation Network

OEA – Organização dos Estados Americanos

TCP – Transmission Control Protocol, Protocolo de Controle de Transmissão

UNIVAC – Universal Automatic Computer, Computador Automático Universal

USENET – Unix User Network

SUMÁRIO

1 INTRODUÇÃO

Não há dúvidas quanto aos benefícios trazidos com a evolução tanto do computador como da internet, de tal maneira que na atualidade é difícil de pensar na ausência de ambos.

Através da Internet as pessoas conseguiram uma nova forma de comunicação, além de um novo modo de comercializar serviços e produtos que são entregues em qualquer lugar do mundo. Essas Vantagens fazem com que o número de pessoas e companhias que adquirem o acesso à internet aumente a cada dia que passa.

Entretanto, com a facilidade de acesso aos meios acima citados, muitas pessoas os usam de forma que violem os direitos de outras, quais sejam praticando crimes virtuais.

Estes delitos são praticados com frequência devido à rapidez com que eles podem ser realizados, em decorrência da dificuldade de encontrar o autor do ilícito e em razão do aperfeiçoamento constante deste na medida em que o Direito e as autoridades policiais apresentam uma evolução mais lenta para o combate destas condutas delituosas.

Levando-se em consideração que esses crimes de informática evoluem conforme ocorrem os avanços tecnológicos, existe uma grande necessidade de progresso do Direito e das autoridades policiais, bem como das ferramentas utilizadas por estes, para que tais criminosos possam ser adequadamente punidos.

Sendo assim, o presente trabalho se propõe a demonstrar quais são os maiores problemas encontrados ao tentar combater os delitos cibernéticos, tendo em vista a enorme dificuldade encontrada pelas autoridades para punir adequadamente as condutas delituosas que muitas vezes acabam impunes sem que o seu autor seja identificado.

Convém analisar inicialmente os fatos antecedentes aos crimes cibernéticos: a evolução do computador, da internet e o surgimento dos crimes

virtuais, bem como a sua conceituação, classificação, o bem jurídico que é tutelado e os seus sujeitos ativo e passivo.

Em seguida o presente trabalho trata da questão dos programas que invadem os computadores, sendo eles os Vírus, Worms, Bots, Trojans, Spywares, Keyloggers e Screenloggers e das condutas delituosas praticadas na internet como os crimes contra a honra, contra a liberdade individual, contra o patrimônio, contra os costumes, os de invasões de privacidade e de lesões a Direitos Humanos.

E por fim, discorre a respeito das maiores dificuldades encontradas para o combate dos crimes de informática sendo elas a formação precária dos policiais, a dificuldade de identificação do autor de um delito cibernético e o aperfeiçoamento deste, a insuficiência de órgãos investigativos no país, a precariedade das ferramentas investigativas, as críticas negativas sobre a Lei 12.737 de 2012 e as questões a respeito da competência de um delito cibernético.

No presente trabalho, para o estudo das premissas dos delitos na informática, é utilizado o método histórico, o qual se procede por meio do recolhimento das fontes de informação necessárias à análise histórica das evoluções e revoluções que foram responsáveis pelos ilícitos citados.

Em seguida, o método utilizado é o dedutivo. Se valendo de bases racionais, partiremos de assuntos gerais para assuntos específicos.

Dessa forma, analisaremos do geral para o específico, do surgimento do computador e da internet até as dificuldades encontradas para combater os crimes praticados pelo seu mau uso.

Em relação aos recursos que serão aproveitados, encontram-se as doutrinas, legislações pertinentes ao tema, bem como a internet.

2 EVOLUÇÃO HISTÓRICA

Não há que se falar em crimes virtuais sem a existência do computador, portanto, é de suma importância realizar a apresentação dos aspectos históricos da invenção tanto do computador como da Internet.

2.1 Breve Histórico Sobre o Computador

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.

Não seria possível falar sobre os crimes virtuais sem antes mencionar o computador, máquina essencial para a realização de muitas atividades cotidianas das pessoas, pois é por meio deste instrumento que se envia, recebe dados e que a grande maioria dos crimes virtuais acontece.

Não foi recente a vontade do homem de criar ferramentas que pudessem auxiliar no cotidiano das pessoas. Sendo assim, o primeiro importante instrumento criado foi o ábaco, na atual região da China, por volta de 3.500 A.C. (ROSSINI, 2004, p. 23)

Outras ferramentas que antecederam a criação do computador merecem destaque, quais sejam os bastões, a máquina calculadora, a máquina analítica e a máquina de recenseamento.

Os bastões são utensílios responsáveis pela computação de dados e foram criados em 1614 pelo escocês John Napier, posteriormente estes bastões evoluíram para os chamados Círculos de Proporção de Willian Oughtred. (ROSSINI, 2004, p. 23-24)

Em seguida, outro importante utensílio foi inventado, sendo ele a máquina de calcular que contribui de forma significativa para a vida da população, facilitando as atividades rotineiras que envolvem cálculos.

Segundo Augusto Eduardo de Souza Rossini (2004, p.24), a máquina calculadora, também denominada máquina aritmética de Pascal, nada mais é do que um instrumento responsável pela realização de cálculos numéricos e foi criada em 1642 por Blaise Pascal, quando este tinha apenas 19 anos.

Após, surgiu um aparelho que contribuiu significativamente para que o computador fosse inventado, trata-se da máquina analítica que devido aos seus aspectos peculiares merece ser mencionada.

A máquina analítica é capaz de fazer operações matemáticas, realizar a impressão dos resultados obtidos e armazenar números, ela teve o seu projeto desenvolvido no ano de 1822 pelo inglês Charles Babbage. (ROSSINI, 2004, p. 24)

Importante ressaltar, a criação da máquina de recenseamento que está entre as ferramentas precursoras do computador e que proporcionou um importante avanço tecnológico para a época.

A máquina de recenseamento constitui um utensílio responsável por fazer o levantamento da população de um município, estado, país, a contagem dos votos de uma eleição, entre outras utilidades, foi criada em 1880 pelo Herman Hollerith com o objetivo de apurar o censo dos Estados Unidos. (ROSSINI, 2004, p. 24)

Não existe uma certeza quanto a quem inventou o computador atual, mas não há dúvidas de que o seu aperfeiçoamento aconteceu devido ao elevado desenvolvimento tecnológico ocorrido no campo da computação durante a Segunda Guerra Mundial.

Corroborando esse entendimento Augusto Eduardo de Souza Rossini (2004, p. 24):

> Não é pacífica a paternidade do moderno computador, ora se dizendo que fora criado por Howard H. Aiken em 1937, ora se afirmando que fora criado por Atasanoff e Berry em 1940. O que fica, entretanto, é que a evolução dessa tecnologia deveu-se ao advento da Segunda Guerra Mundial, que gerou, além de grande desgraça, enorme avanço tecnológico nas mais variadas áreas, inclusive na computação.

Portanto, fica evidenciado que apesar das inúmeras perdas e destruições, a Segunda Guerra Mundial trouxe avanços na tecnologia de diversos campos.

Com base em Carlos Alberto Rohrmann (2005, p.2), os computadores digitais originaram do estudo da álgebra digital, sendo conhecida também por Álgebra de Boole, e apareceram na década de 1940, tendo o seu procedimento baseado no tratamento e na representação das informações em somente duas variáveis, zeros e uns.

Assim, o computador digital foi inventado em virtude de pesquisas realizadas no campo da álgebra digital.

Em 1847, o matemático inglês, George Boole iniciou o estudo da álgebra que leva o seu nome tendo como base as duas variáveis que são utilizadas nos computadores digitais. (ROHRMANN, 2005, p. 2)

Sendo assim, a álgebra recebeu o nome desse matemático, porque ele começou as suas pesquisas contribuindo significativamente para que o computador digital fosse inventado.

No ano de 1951, o primeiro computador comercial foi espalhado no mercado com o nome de UNIVAC, tendo como objetivo realizar o censo dos Estados Unidos e é importante destacar que até este momento os computadores possuíam cerca de 18 mil válvulas e pesavam aproximadamente 30 toneladas. (ROHRMANN, 2005, p. 2)

Deste modo, fica evidente que o aparelho computador até esse momento não era acessível para a população, devido ao seu tamanho e peso, sendo somente utilizado para fins de pesquisas por parte do governo americano.

Conforme Carlos Alberto Rohrmann (2005, p. 2), a grande novidade mesmo aconteceu em 1971 com a criação dos microprocessadores, que receberam o nome de computadores pessoais e pela primeira vez o computador passou a caber nas mesas de trabalho, tendo este fato contribuído para a sua popularização.

E por fim, com relação à evolução do computador é importante ressaltar que existem cinco gerações de computadores.

Sendo que a Primeira Geração trouxe como novidade os computadores à base de válvulas a vácuo; a Segunda Geração substituiu as válvulas por transistores; a Terceira Geração substituiu os transistores pelos circuitos integrados; a Quarta Geração substituiu os circuitos pelos microprocessadores e a Quinta Geração trouxe um enorme avanço para a computação.

A respeito das gerações de computadores:

> 1ª geração (de 1940 a 1952) – computadores à base de válvulas à vácuo – alimentação por cartões perfurados – uso exclusivamente militar (nessa época surgiu a teoria da "informática jurídica" desenvolvida por Lee Loevinger). 2ª geração (de 1952 a 1964) – substituição das válvulas por transistores – maior velocidade – uso administrativo e gerencial. 3ª geração (de 1964 a 1971) – substituição dos transistores pelos circuitos integrados (surgidos em 1964) – miniaturização dos grandes computadores – evolução dos softwares e criação dos chips de memória – ampliação do uso comercial. 4ª Geração (de 1971 a 1981) – substituição dos circuitos pelos microprocessadores – criação dos floppy disks, ou disquetes, para o armazenamento de dados – nascimento da telemática. 5ª geração (de 1981 até hoje) – enorme avanço da computação – criação da inteligência artificial, da linguagem natural e da altíssima velocidade do processamento de dados – principal novidade: disseminação da internet. (ROSSINI, 2004, p.25)

Não existem dúvidas de que com os avanços tecnológicos não só computadores, mas outras máquinas mais evoluídas ainda estão por vir.

2.2 Breve Histórico Sobre a Internet

Antes de tudo é importante tratar da conceituação da internet para o melhor entendimento do presente trabalho, porque a maioria das pessoas sabem os benefícios trazidos pelo seu uso, mas não sabem precisamente o conceito.

Citando a Liliana Minardi Paesani (2000, p.27), pode-se conceituar a internet como:

> O que é a Internet? A resposta não é clara nem completa. Sob o ponto de vista técnico, a Internet é uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites. Sua difusão é levemente semelhante à da rede telefônica. Existe, entretanto, uma radical diferença entre uma rede de computadores e uma rede telefônica: cada computador pode conter e fornecer, a pedido do usuário, uma infinidade de informações que dificilmente seriam obtidas por meio de telefonemas.

Portanto, é de suma importância saber o conceito da internet, para entender a diferenciação entre uma rede de computadores e uma rede telefônica, tendo em vista que os computadores podem fornecer e armazenar dados, o que não acontece em uma rede de telefones.

Durante a Guerra Fria no ano de 1962, houve a necessidade do governo norte americano de criar uma rede conectada, com o objetivo de que esta não fosse interrompida caso os Estados Unidos sofresse algum ataque nuclear. (ROSSINI, 2004, p.26)

Assim, fica evidente que um dos objetivos da invenção da internet foi atender as necessidades do governo americano de manter comunicação através de computadores durante as guerras.

Ideias foram apresentadas no ano de 1967, porém foi somente em 1968 com a criação da ARPANET que as primeiras premissas da atual internet surgiram. (ROSSINI, 2004, p.26)

Assim, fica claro que o surgimento deste plano foi essencial para que a rede de computadores conectados fosse inventada.

Mas foi somente em 1969 que a Internet foi criada, através do projeto ARPANET:

> O projeto Arpanet da agência de projetos avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, à Rand Corporation a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos. A solução aventada foi a criação de pequenas redes locais (LAN), posicionadas nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (WAN). Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, essa rede de redes conexas – Internet, isto é Inter Networking, literalmente, coligação entre redes locais distantes, garantiria a comunicação entre as remanescentes cidades coligadas. (PAESANI, 2000, p.25)

De acordo com o Carlos Alberto Rohrmann (2005, p.5), muito tempo antes do nascimento da ARPANET, já haviam estudos avançados com redes de computadores na Universidade de Los Angeles e no Massachussets Institute of Technology, logo, não condiz com a verdade alegar que a internet teve sua origem unicamente no campo militar.

Portanto, as Universidades também contribuíram de forma significativa para que a Internet fosse criada.

Na década de 70, muitos acontecimentos importantes ocorreram:

> Em 1971, a rede cresceu e foram abrangidas agências governamentais e militares norte-americanas, incluindo a NASA. Em 1972 foi lançado o primeiro programa de correio eletrônico (e-mail) e, em 1973, foram estabelecidas as primeiras conexões internacionais, interligando-se Estados Unidos da América, Reino Unido e Noruega. Em 1974 foi lançado o primeiro serviço comercial de transmissão de dados, nada mais do que uma versão comercial da ARPANET. Em 1976 foram incorporadas conexões de rádio e satélite e em 1979 foi criada a Usenet, que era uma rede descentralizada de grupos de notícias. (ROSSINI, 2004, p. 26)

Logo, merece destaque o lançamento do primeiro programa de correio eletrônico nesta década, serviço que ainda é muito utilizado no mundo inteiro e o estabelecimento das primeiras conexões internacionais que contribuíram para a ampliação do serviço de Internet.

No final da década de 70 e início da década de 80, a internet nos Estados Unidos era utilizada somente para fins militares e universitários, ao passo que na mesma época na França, nasceu o primeiro sistema telemático de utilização para fins comerciais, através da rede Minitel. (ROSSINI, 2004, p.26)

Sendo assim, a França deu o primeiro passo para que a Internet deixasse de ser usada somente por pessoas específicas e passasse a ser utilizada por toda a coletividade.

A Minitel usava a rede telefônica para alcançar um elevado número de usuários e foi criada pela France Telecóm, por meio dela, a internet passou a ter utilidade para transmissão de mensagens, jogos, entre outras serventias. No entanto, esta conexão não saiu da França, devido ao grande custo necessário para ser mundialmente utilizada e por causa das suas particularidades técnicas, que não eram compatíveis com o restante do mundo. (ROSSINI, 2004, p.26-27)

Deste modo, apesar da Minitel não ter saído da França, não há dúvidas da imensa importância desta, tendo em vista que ela trouxe a ideia de uma popularização da Internet, para que esta fosse utilizada para comunicação, lazer e não somente em situações de guerra ou com a finalidade de pesquisas acadêmicas.

Segundo Augusto Eduardo de Souza Rossini (2004, p.27) nos anos 80 merece destaque:

> Entretanto, foi na década de 80 que ocorreu a transição da citada ARPANET para o que atualmente se denomina Internet. Em 1982 foi estabelecido o padrão IP/TCP, até hoje usado na rede, tornando-se obrigatório em 1983 e, somente nesse momento, pôde-se conceituar a Internet como um conjunto de redes interligadas. Interessa destacar que nessa mesma época surgiu o conceito de hacker, a denominação ciberespaço [...] e tantas outras terminologias até hoje utilizadas. Evidencia-se, pois que alguns conceitos que surgiram nesse momento histórico são até hoje usados por milhões de pessoas e foram aproveitados pelo próprio Direito Penal. Em 1984, a ARPANET foi dividida em duas redes: a Milnet (Militar) e a Arpanet (acadêmica), ambas sob o controle do Departamento de Defesa dos Estados Unidos. Neste mesmo ano foi criado o sistema de nomes e domínios, que substituiu o sistema numérico, permitindo-se dessa maneira, o acesso mais rápido a outros servidores, sem a necessária memorização de grandes códigos numéricos. Em 1985 foi criada a NSFNET e foram estabelecidos cinco centros de supercomputação, o que permitiu uma explosão de conexões, notadamente nas universidades, permitindo-se, nesse momento, o desenvolvimento da estrutura do que hoje é a Internet. Em 1988, Dinamarca, Finlândia, Canadá, Islândia, França, Suécia e Noruega foram interligados a NSFNET e tais conexões restringiam-se ao campo universitário, podendo-se afirmar que nesse instante se estabeleceu o núcleo da atual Internet. Em 1989 aderiram a NSFNET, a Austrália, Alemanha, Israel, Itália, Japão, México, Holanda, Nova Zelândia, Reino Unido e Porto Rico. Neste ano, o número de servidores chegou a cem mil e ocorreu a primeira experiência de correio eletrônico comercial.

Assim sendo, os anos oitenta foram de enormes avanços na história da Internet, sendo importante destacar que foi estabelecido o padrão IP/TCP que ainda é o nosso modelo usado e a criação de terminologias que permanecem atuais, além da invenção da NSFNET que proporcionou a ampliação das conexões, fazendo com que diversos países aderissem essa rede e ocasionando a estruturação da atual Internet.

E por fim, conforme Augusto Eduardo de Souza Rossini (2004, p.27-29) na década de 90 vale ressaltar:

> Em 1990, a Arpanet foi desativada pelo Departamento de Defesa, sendo substituída pelos backbones da NSFNET [...] Neste ano, o Brasil também foi conectado a NSFNET, bem como Argentina, Áustria, Bélgica, Chile, Grécia, Índia, Irlanda, Coréia do Sul, Suíça e Espanha. Em 1991, o governo norte-americano criou o NREN (National Research and Education Network) com a função de conduzir o tráfego de alta velocidade para fins de pesquisa, sem qualquer finalidade comercial. Redes privadas foram conectadas a Internet. Nesse mesmo ano, praticamente todos os países da Europa Ocidental também se integraram à rede, o mesmo ocorrendo com Hong Kong, Portugal, Cingapura, África do Sul, Taiwan, Tunísia, Croácia, República Checa, Hungria e Polônia. E surgiram os grandes provedores da Internet.

> Em 1992 foi implementada a primeira ferramenta de busca e se integraram à rede Venezuela e Equador. Em 1993 muitos sites importantes foram criados, v.g. o da Casa Branca, o das Nações Unidas e o do Banco Mundial. Aderiram à rede, Costa Rica, Peru, Colômbia, Nicarágua, Panamá, Uruguai, Rússia, Ucrânia e China. Em 1994 surgiram serviços de entrega pela rede (Pizza Hut), o primeiro banco on-line e os primeiros shoppings virtuais. Em 1995, a Internet foi privatizada, com o estabelecimento de provedores independentes. No Brasil, a Embratel deixou de ter o monopólio das transmissões. [...] O ano de 1996 caracteriza-se pela primeira iniciativa de controle oficial do uso da Internet, tendo o Congresso Norte Americano tentado proibir a distribuição de material pornográfico através da rede, tendo, contudo, a Suprema Corte daquele país considerado a lei inconstitucional. Em 1997 houve a ampliação dos conflitos legais advindos do uso da rede. [...] Em 1998, a Organização Mundial do Comércio (OMC) avaliou que os negócios na rede atingiram 300 bilhões de dólares; foram criados os notebooks; e surgiram os provedores gratuitos, praticamente desaparecidos nos dois anos seguintes. De 1999 até hoje a Internet somente cresceu, chegando a bilionários patamares, permitindo-se concluir que já faz parte do cotidiano de uma grande parcela da sociedade moderna. Aliás, é desta época a estruturação da Internet Rápida, também chamada de Banda Larga, que agiliza sobremaneira o acesso e, portanto, potencializa seu uso.

Portanto, na década de 90 merece mencionar que o Brasil aderiu a NSFNET, houve a implementação da primeira ferramenta de busca na Internet, serviços de entrega foram criados, assim como bancos on-lines e lojas virtuais, também ocorreu o aumento de conflitos legais devido à utilização da rede e a criação da Banda Larga, que possibilita um acesso bem mais rápido da Internet.

Atualmente, a internet é uma ferramenta indispensável, porque através dela podem ser realizadas compras, transações bancárias, pesquisas, manter contato com os amigos e familiares, ou seja, é difícil imaginar o cotidiano das pessoas sem a utilização da internet, tendo em vista que esta colaborou para o processo de globalização e unificação dos “mundos”.

2.3 Breve Histórico Sobre os Crimes Virtuais

O surgimento dos crimes virtuais ocorreu na década de 60, estes delitos versavam sobre o infrator sabotar, manipular, espionar ou exercer uso abusivo de computador ou sistema.

Em 1980, na medida em que ocorreram os avanços tecnológicos, os crimes na internet também evoluíram e aumentaram significativamente, os crimes

mais frequentes passaram a ser pornografia infantil, pirataria de programas, manipulações de caixas bancários e abusos de telecomunicação.

Tendo em vista que a internet somente chegou ao Brasil em 1990, os crimes cibernéticos surgiram no país apenas no final da década de 90, sendo que desta época em diante, as pessoas passaram a ter o conhecimento da existência desses ilícitos e foi o início das constantes preocupações governamentais quanto aos crimes virtuais.

Com o passar dos tempos às tecnologias foram avançando cada vez mais e na mesma medida que a internet se tornava mais popular, os cibercrimes também cresciam, levando em consideração que as legislações ficavam cada vez mais ultrapassadas e que os sistemas de defesa não eram tão eficientes.

Corroborando esse entendimento Mauro Marcelo de Lima e Silva (2000):

> Aqui no Brasil, como não poderia ser diferente, existe um absoluto despreparo, ignorância e falta de visão herdados por uma geração de policiais no melhor estilo old dinosaurs que nem sabem para que serve um mouse de computador.

Atualmente, esses problemas ainda existem como exemplo da precariedade da legislação, merece destaque que embora a internet tenha surgido no país em 1990, somente em 2013 foram tipificadas algumas condutas delituosas ocorridas neste meio, e ainda existem muitos policiais que não são devidamente treinados para identificar os autores, além de não existirem ferramentas adequadas disponíveis para a identificação destes delitos.

A demora na tipificação dos crimes virtuais ocorreu, porque muitos operadores do direito consideraram que as legislações já existentes, como a do Código Penal eram suficientes para punir as práticas destes delitos, o argumento utilizado por eles para sustentar este posicionamento era que os ilícitos cometidos já estavam presentes nas leis brasileiras, como a injúria, a calúnia e a difamação, por exemplo, alegavam que somente o instrumento para a prática desses ilícitos que era diferente, no caso o computador.

Entretanto, estes operadores do direito estavam enganados, pois em maio de 2012 ocorreu um crime cibernético com uma famosa atriz global, Carolina

Dieckmann, quando ela teve o seu computador invadido e fotos íntimas publicadas na internet, sendo inclusive chantageada para evitar que essas imagens fossem colocadas na rede, este acontecimento agilizou e muito a situação da ausência de tipificação destas condutas, já que no dia 02 de abril de 2013, entrou em vigor a lei que tipifica diversas condutas de crimes cibernéticos.

Portanto, fica evidente que com relação à punição aos crimes virtuais, a situação no país ainda precisa melhorar e muito, sendo necessária uma melhoria tanto na estrutura do país, quanto na capacitação dos policiais e dos demais profissionais que auxiliam no combate a esses delitos, bem como um progresso na ferramenta utilizada por estes e o aumento dos órgãos investigativos para atender a demanda adequadamente.

3 CRIMES VIRTUAIS

O aumento do uso de computadores, smartphones e tablets nos últimos anos, assim como a facilidade de acessar a internet, proporcionam um indiscutível avanço para a população e facilitam a realização de várias atividades cotidianas de um modo mais simples e rápido, entretanto, todos estes fatores contribuíram significativamente para uma nova forma de prática criminal: os crimes virtuais.

Sendo assim, é extremamente relevante estudar de modo mais aprofundado esses novos delitos que surgiram.

3.1 Conceito

As designações a respeito dos delitos que possuem relação com as tecnologias avançadas são variadas: cibercrimes, delitos cibernéticos, crimes virtuais, criminalidade mediante computadores, criminalidade de computador, delito informático, delinquência informática, crimes de internet, entre outras denominações.

Apesar de todos esses termos serem referentes à mesma conduta criminosa, alguns autores preferem a denominação delitos informáticos, por esta possuir uma maior abrangência, que compreende um campo de pesquisa maior, sendo assim considerada toda conduta delituosa que possuir relação com a computação e as novas tecnologias.

Corroborando esse entendimento Augusto Eduardo de Souza Rossini (2004, p.110):

> A denominação “delitos informáticos” alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível “conexão” à Rede Mundial de Computadores, ou qualquer outro ambiente telemático.

> Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou "delitos informáticos".

Conforme LIMA (2006) *apud* FIORILLO e CONTE (2013, p.143), os crimes de computador são definidos como:

> Qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta.

Deste modo, se o computador for usado de alguma maneira na conduta de uma pessoa que realiza uma ação ou omissão, desde que presentes os elementos tipicidade, antijuridicidade e culpabilidade, essa pessoa estará praticando um crime virtual.

Segundo Augusto Eduardo de Souza Rossini (2004, p.40), um dos melhores conceitos de delitos cibernéticos é o realizado pela Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas em 1983: "o crime de informática é qualquer conduta ilegal, não ética, ou não autorizada que envolva processamento automático de dados e/ou a transmissão de dados".

Já o secretário executivo da Associação de Direito e Informática do Chile, MANZUR (2000) *apud* FIORILLO e CONTE (2013, p.143) conceituou estes crimes de forma mais complexa:

> Todas aquelas ações ou omissões típicas, antijurídicas e dolosas.
> Trata-se de fatos isolados ou em série, cometidos contra pessoas físicas ou jurídicas, realizadas com o uso de um sistema de tratamento da informação e destinadas a produzir prejuízos para a vítima, através de atentados à saúde técnica informática, a qual, geralmente, produzirá de maneira colateral lesões a diversos valores jurídicos, ocasionando, muitas vezes, um benefício ilícito ao agente, seja patrimonial, ou não, atue ele com ou sem ânimo de lucro.

E por fim, "em outras palavras, podemos considerar como crimes informáticos os ilícitos perpetrados por intermédio da Internet ou com o auxílio desta, causando algum tipo de dano à vítima". (FIORILLO E CONTE (2013, p.143)

Sendo assim, mesmo havendo diversos conceitos para essa prática delituosa, ela sempre será exercida por meio de um computador (agora por meio também do tablet ou smartphone) e não precisa necessariamente que essas condutas sejam realizadas através da internet, embora a grande maioria seja efetivada nesse meio.

3.2 Classificação

Diversas são as formas utilizadas para classificar os delitos de informática, porém merecem destaque, as classificações citadas a seguir.

Uma das classificações faz a distinção entre os delitos que usam o computador como um meio para a prática criminal e aqueles que utilizam o computador como um alvo do ato criminoso. Essa forma de distinguir os delitos origina a classificação destes em crimes próprios ou puros e os crimes impróprios ou impuros.

Os crimes próprios ou puros são aqueles realizados com o uso dos sistemas de computadores, mesmo se tratando de um computador simples que não esteja interligado em alguma rede de computadores. Para exemplificar esses crimes, podemos citar a obtenção de senhas de um computador e a invenção e a disseminação de vírus e outros programas maliciosos para o computador como o caso dos cavalos de tróia.(ROHRMANN, 2005, p. 121)

Portanto, os crimes próprios ou puros tratam-se daqueles praticados utilizando computador, esteja este conectado com a internet ou não.

Já os crimes impróprios ou impuros são aqueles que não dependem da utilização dos computadores e dos demais sistemas eletrônicos para serem praticados. Sendo assim, esses sistemas são utilizados somente na prática da conduta delituosa e os resultados alcançados vão além do computador que por muitas vezes nem apresenta a sua tutela jurídica ameaçada. Como exemplo destes crimes, é importante mencionar os crimes contra a honra realizados através dos sistemas eletrônicos; os crimes de estelionato e a conduta de ameaçar uma pessoa

utilizando algum modo de conversação pela internet. (ROHRMANN, 2005, p. 121-122)

Outra classificação é compreendida nos casos em que existe o uso do computador para a prática do ilícito penal, assim como as condutas delitivas contra o computador ou com base nas informações contidas neste. Sendo assim, os crimes de informática são classificados em puros, mistos e comuns.

Os crimes virtuais puros são aqueles em que o objetivo é atingir o computador, o sistema de computação ou os dados e as informações nele contidas. Para exemplificar, podemos mencionar os crimes que atacam os programas informáticos, conhecidos como softwares, e aqueles que atacam a parte física do computador, sendo esta conhecida como hardware. (FIORILLO e CONTE, 2013, p. 145)

Conforme essa classificação, os crimes virtuais puros são aqueles que apresentam a finalidade de atingir qualquer componente do computador (esteja o elemento dentro dele ou não) e de lesionar o sistema de computadores.

Os crimes mistos são aqueles em que o autor do delito não objetiva atingir o sistema de computação e seus componentes, entretanto, a cibernética é um instrumento essencial para que a ação delinquente seja consumada. Temos como exemplo a transferência ilícita de valores em uma homebanking (consiste em um serviço prestado pelos bancos que possibilita efetuar transações bancárias através da internet, tendo o cliente o acesso a uma página segura da instituição bancária). (FIORILLO e CONTE, 2013, p. 145)

Deste modo, os crimes mistos tratam-se daqueles em que o sujeito ativo não possui o fim de atingir os componentes do computador e o sistema de computadores, mas a Internet é o meio imprescindível para que os fatos típicos sejam praticados, sem esta não seria possível a realização das condutas criminosas.

Os crimes comuns são aqueles em que o sujeito ativo não apresenta a finalidade de atingir o sistema de informática ou seus componentes, mas este usa a computação como um instrumento para a prática da ação, sendo que a computação nesse caso, não é fundamental para a realização desse ilícito, poderia ser realizado por outro meio. Como exemplo podemos citar os crimes contra a honra, o crime de estelionato e ameaça. (FIORILLO e CONTE, 2013, p. 145)

Embora existam diversas formas de classificação desses crimes virtuais, estas são usadas meramente para fins didáticos e a tendência delas é se tornarem ultrapassadas na medida em que o Direito passa por avanços.

3.3 Bem Jurídico Tutelado

Antes de adentrarmos nos aspectos mais discutidos sobre os bens jurídicos, convém conceituarmos estes.

Os bens são valores fundamentais para que a sociedade se mantenha harmonizada e estes estão diretamente ligados a essa finalidade. Possuem sua importância reconhecida pelo Estado que passa a exercer a sua tutela de forma jurídica, transformando-os assim, em bens jurídicos.

O que podemos notar nos delitos informáticos é que estes afetam diversos bens jurídicos. O autor do delito pode atuar contra o sistema informático, gerando um dano contra o hardware (parte física do computador ou dos dispositivos móveis) ou contra o software (programas de computador ou de dispositivos móveis) ou pode atuar contra a informação contida no computador ou nos aparelhos móveis (smatphones, tablets, iphones, ipads) ocasionando uma intranquilidade da população.

Quando o sujeito ativo realiza uma conduta delituosa por meio de um dispositivo eletrônico, deve ser observado sobre qual objeto de tutela incidiu o efeito do dano. Se o autor utilizar o aparelho eletrônico para realizar a calúnia de uma pessoa, o bem jurídico atingido será a honra objetiva; agora se este realizar uma ameaça através do whatsapp (aplicativo que possibilita a troca de mensagens pelo celular sem realizar o pagamento por sms, apenas utilizando a internet), o bem jurídico violado será a liberdade individual da vítima.

Então, nos crimes praticados com a utilização do sistema informático, onde este é apenas um meio para a prática criminosa, poderá ocorrer uma violação do patrimônio, da honra, da liberdade individual, entre outros direitos, e estes serão os bens jurídicos tutelados respectivamente. Sendo assim, haverá a proteção do

bem jurídico tutelado pelo código penal e que seja correspondente à lesão ocasionada pelo comportamento do sujeito ativo.

Com a criação da lei 12.737 de 2012, popularmente conhecida como Lei Carolina Dieckmann, foram incluídos no Código Penal os artigos 154-A e 154-B e foram alterados os artigos 266 e 298 do mesmo código, sendo estes dispositivos legais responsáveis pela tipificação dos delitos virtuais.

O artigo 154-A do Código Penal trata da invasão de dispositivo informático:

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

Essa lei veio com o objetivo de tutelar o bem jurídico da liberdade individual e do direito ao sigilo pessoal e profissional devido à importância desses bens jurídicos para a convivência em sociedade.

Portanto, o fator determinante para saber qual o bem jurídico tutelado nesses delitos cibernéticos é verificar a forma como esse ilícito é praticado, se for crime próprio este se encontra tipificado no Código Penal e o bem jurídico tutelado será a liberdade individual e o direito ao sigilo pessoal e profissional; se for crime impróprio, esse apresentará o bem jurídico tutelado pela norma prevista na lei que corresponda ao dano causado pelo delito.

3.4 Sujeito Ativo

Na maioria dos casos, os delitos informáticos são praticados por pessoas que possuem um imenso conhecimento sobre tecnologia, informática, sistemas, mas não podemos generalizar, porque qualquer pessoa que apresente conhecimentos básicos sobre esses assuntos é plenamente capaz de cometer algum ilícito virtual.

Levando em consideração que a rede mundial de computadores apresenta uma língua distinta, caracterizada pelo uso frequente das palavras em inglês, em se tratando da denominação dos sujeitos ativos não seria diferente.

Os agentes causadores desses crimes cometidos na internet são: os hackers, crackers, phreakers, cardes, cyber terroristas, spammers, pichadores virtuais, lammers, wannabes, arackers e gurus.

Muitas pessoas possuem o pensamento errôneo de que quem pratica crimes virtuais é chamado de hacker, portanto, é de suma importância saber os aspectos peculiares de cada sujeito ativo desses crimes.

> HACKER - Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hackers para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas, etc.
> CRACKER – Este indivíduo usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática pra causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos, etc.
> PHREAKER – Este indivíduo é o terror das companhias telefônicas, pois são especialistas em burlar sistemas de telefonia, fixa ou móvel. Os prejuízos são enormes e incalculáveis.
> SPAMMERS – São pessoas e empresas que enviam e-mails indesejados, muitas vezes lotando sua caixa de e-mails com pornografia, propaganda, lançamento de produtos, assinatura de alguma revista, convite para danceterias e bailes, etc. São os chamados SPAMS – e-mails não solicitados. Um levantamento feito mostra que mais de 60% dos e-mails recebidos atualmente em nossa caixa postal são spams e a maioria ou contém vírus ou algum tipo de propaganda. Dados de janeiro de 2008 apontam o Brasil como o 4º país no mundo que mais envia spams!
> PICHADORES VIRTUAIS – Estes adoram violar algum site, a maioria do poder público, como do FBI, Pentágono, Supremo Tribunal Federal, INSS, e lá deixar sua marca, às vezes acontece algum tipo de protesto político ou religioso com esse tipo de invasão, ou podemos chamar de “manifesto”, normalmente não causam danos.
> CYBER TERRORISTA – Difunde o terror, o medo e faz apologia ao terrorismo e ataques em massa, estes muitas vezes com cunho religioso ou protesto contra alguma potência. (NOGUEIRA, 2008, p.61-62)

Portanto, fica evidente a utilização de forma errônea do termo hacker, tendo em vista que este possui um grande conhecimento de informática e costuma invadir sites, mas apenas com o objetivo de demonstrar como as pessoas estão desprotegidas na Internet ou para provar que consegue entrar em certa página, já o

cracker apresenta uma imensa noção de informática também, mas ele usa o que sabe para praticar crimes na Internet, causando danos para suas vítimas e obtendo vantagens ilícitas com suas condutas.

O Phreaker é responsável por fraudar o sistema telefônico; o Spammer é a pessoa ou empresa que constantemente envia e-mails não solicitados; já o Pichador Virtual consiste naquele indivíduo que não possui o hábito de causar prejuízos, mas gosta de invadir páginas do governo, algumas vezes com o objetivo de realizar protestos religiosos ou políticos e por fim, o Cyber Terrorista é aquele sujeito que pratica o terrorismo na internet e realiza ataques em massa de caráter religioso ou para protestar contra uma nação.

Conforme o BARROS (2007) *apud* FIORILLO e CONTE (2013, p. 153):

> Cardes é a denominação que se dá aos criminosos que se apropriam do número de cartões de crédito, obtidos através de invasão de listas eletrônicas constantes nos sites de compras efetivadas pela Internet, ou de outros meios ilícitos para realizar toda a espécie de compras.
> Eles conhecem o número dos cartões de crédito dos usuários da rede, normalmente a partir da instalação de programas espiões, capazes de permitir o acesso a todo tipo de informação digitada no teclado do computador do usuário.
> Já denominação cyberterrorists indica a atividade ilícita daquele que desenvolve bombas lógicas ou vírus com o intuito de sabotar computadores e provocar a queda do sistema de grandes provedores, impossibilitando o acesso de usuários, gerando grandes prejuízos econômicos.

Deste modo, os Cardes descobrem os números de cartões de crédito das pessoas por meio de programas maliciosos que permitem que eles vejam tudo que está sendo digitado no teclado do computador da vítima, assim quando esta realiza alguma compra em lojas virtuais e digita o número de seu cartão, os criminosos possuem acesso a ele; já os cyberterrotists criam programas mal intencionados para derrubar o sistema de Internet dos grandes servidores, deixando as pessoas sem acesso a rede.

Fabrízio Rosa (2002, p. 59 e 60) faz importantes observações a respeito dos sujeitos ativos:

> Uma figura que é muito comentada como sendo criminoso de computador é o hacker. Entretanto, no ambiente informático é bom esclarecer e melhor definir essa figura. Senão vejamos:
> - hacker: é aquele que tem conhecimentos profundos de sistemas operacionais e linguagens de programação, principalmente Unix e C.

> Conhece as falhas de segurança dos sistemas e está sempre a procura de novas falhas. Invade sistemas pelo prazer de provar a si mesmo que é capaz, sem alterar nada;
> - cracker: o mesmo que o hacker, com a diferença de utilizar seu conhecimento para o "mal". Destruir e roubar são suas palavras de ordem. Assim, o cracker usa seus conhecimentos para ganhar algo; rouba informações sigilosas para fins próprios e destrói sistemas para se exibir;
> - phreaker: especializado em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros;
> - lammer: é quem está tentando ser hacker, [...] possui um pouco de conhecimento sobre invasão de sistemas e fica se exibindo na internet por causa disso. É o iniciante;
> - wannabe: é o principiante que já aprendeu a usar os programas prontos dos hackers;
> - aracker: são os chamados hackers de araque. [...];
> - guru: [...] É aquele que tem conhecimentos superiores e grande domínio sobre todos os tipos de sistemas.

Assim sendo, fica evidente a utilização de forma errada da terminologia hacker por diversas pessoas e demonstra os diferentes tipos de autores dos delitos de informática.

3.5 Sujeito Passivo

Sujeito passivo é a pessoa que teve o seu bem jurídico lesionado ou que sofreu ameaça de lesão a este bem.

Conforme a natureza do delito é que será identificado qual é o sujeito passivo, podendo a vítima ser uma pessoa física ou jurídica, o Estado, a coletividade e a comunidade internacional.

Assim, todo mundo que possui acesso à rede mundial de computadores tem a possibilidade de ser sujeito passivo destes delitos, já que diariamente todos correm risco de cair em diversos golpes, por exemplo, ter o computador invadido ocasionando danos, receber e-mails com ameaças ao computador disfarçadas, ter dados e senhas furtados e quando um agente causador desses crimes tira um site de serviços de um órgão público do ar, esse ato atinge a todos, seja do setor público ou privado, pessoas físicas ou jurídicas.

4 PROGRAMAS INVASORES DE COMPUTADOR

Assim como os sujeitos ativos, os programas invasores de computador apresentam uma denominação distinta, sendo conhecidos como softwares criminosos, códigos maliciosos ou malwares.

As principais causas que levam uma pessoa a espalhar esses programas são para obter vantagem financeira, conseguir informações sigilosas, para se autopromover e por vandalismo.

Esses malwares são rotulados conforme as peculiaridades que apresentam, merecendo destaque os vírus, worms, bots, trojans, spywares, keyloggers e screenloggers que serão analisados com maior profundidade a seguir.

4.1 Vírus

Os primeiros softwares criminosos que surgiram foram os vírus. Sendo que os vírus iniciais foram criados no princípio da década de oitenta e se alastravam através de disquetes infectados fazendo com que as informações de inicialização do computador fossem alteradas.

A partir de então, a sua capacidade destrutiva vem aumentando consideravelmente e para piorar, surgiram novos tipos de vírus: cavalo de tróia, worm, bot e spyware.

De acordo com a Cartilha de Segurança Para Internet (2012, p.24):

> Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado. O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen-drives*.

> Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:
> **Vírus propagado por *e-mail*:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador. **Vírus de *script*:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário. **Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõem o Microsoft Office (Excel, Word e PowerPoint, entre outros). **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M**ultimedia **M**essage **S**ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

Assim, o vírus é um programa invasor que se alastra no computador devido ao fato de fazer cópias dele mesmo e acaba fazendo parte de outros programas e arquivos. Para que ele entre em atividade é necessário que um software ou documento contaminado seja executado. Existe o vírus que fica escondido e danifica os arquivos do disco do computador e realiza diversas atividades sem que o usuário saiba e tem aquele que só se manifesta em datas determinadas, ficando evidente a capacidade destrutiva que um ele possui.

4.2 Worm

O worm é uma modalidade de vírus, ou seja, também é um programa invasor de computador mal intencionado, no entanto, este apresenta algumas peculiaridades que merecem certo destaque.

Os worms são programas que remetem cópias deles mesmos para outros computadores, agindo diferente dos vírus, porque o worm não embute cópias em outros programas e não precisa ser executado para se alastrar. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.25)

Portanto, o worm também realiza cópias dele mesmo, no entanto o que o diferencia do vírus é o fato dele enviar suas cópias para outros computadores ao invés de fazer parte de outros programas e arquivos e outro aspecto peculiar é que ele não precisa ser executado pelo usuário para poder agir.

Eles exploram os aspectos vulneráveis ou as falhas existentes nas configurações de programas instalados nos computadores ou agem através da execução direta de suas cópias. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.25)

Assim, esses programas procuram falhas ou vulnerabilidades em softwares presentes no computador para que possam agir ou atuam por meio da execução automática das cópias que eles criaram.

Os worms são conhecidos por consumir muitos recursos do computador, isso acontece porque eles espalham um enorme número de cópias deles mesmos, fazendo com que o desempenho e utilização da rede e do computador sejam afetados. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.25)

Também são softwares que gozam de autonomia e que são inventados para exercer certas missões como, por exemplo, enviar spams (são mensagens de teor invariável, enviadas de forma exagerada e sem que o destinatário as tenha solicitado) ou atacar sites.

Outra atividade característica deles é a de abrir portas para a entrada de outros worms, possibilitando assim, o acesso destes ao computador.

Portanto, é evidente o caráter nocivo que esse software criminoso apresenta para os computadores que ele invade.

4.3 Bot

O bot trata-se de mais uma categoria de vírus, sendo assim, um programa malicioso que apresenta alguns aspectos distintos merecedores de destaque.

Conforme a Cartilha de Segurança para a Internet (2012, p.26):

> Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam. Um computador infectado por um bot costuma ser chamado de zumbi (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de spam zombie quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam. Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante (com o uso de proxies instalados nos zumbis).

Deste modo, fica claro como o bot pode ser prejudicial para os computadores que são atacados por ele, porque ele explora as falhas nos programas existentes, se alastra de forma automática e permite que o criminoso controle o dispositivo que foi infectado a distância, utilizando ele para a prática de atividades mal intencionadas.

4.4 Trojan ou Cavalo de Tróia

O cavalo de tróia é mais uma modalidade de vírus, sendo um programa invasor de computador que tem por finalidade causar danos, porém apresenta aspectos que o diferem dos outros programas.

O Trojan ou Cavalo de Tróia é um software geralmente recebido como um “presente de grego”, exemplificando, é um programa que pode ser recebido ou obtido em sites, que possui a aparência de um cartão virtual, álbuns de fotos, protetor de tela, jogo, entre outras formas de ludibriar. Normalmente aparece como um arquivo único e precisa que o usuário do computador o execute para que seja instalado. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.28)

Deste modo, o trojan possui como objetivo enganar o usuário do computador, tendo em vista que ele fica escondido em arquivos comuns que normalmente não causariam danos no aparelho, mas a partir do momento que a vítima executa o documento infectado, o cavalo de tróia é instalado.

Mas também pode ser instalado por invasores que fazem alterações em programas que já existem no computador para que estes possam desempenhar as suas tarefas habituais e também executar atos maliciosos. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.28)

Então, outra forma de instalar este software ocorre quando alguém acessa um dispositivo informático e modifica programas existentes nele para que eles realizem suas atividades de costume e simultaneamente causem danos no aparelho.

Além de exercer tarefas para as quais foi aparentemente projetado, executa também outros papéis mal-intencionados e sem que o usuário saiba, como por exemplo, instalar um vírus ou abrir portas que podem ser acessadas à distância por um invasor. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.28)

De tal modo, não restam dúvidas dos malefícios causados pela ação dos trojans nos computadores.

4.5 Spyware

A última categoria de vírus é o spyware que tem como objetivo controlar as atividades desempenhadas em um computador e mandar os dados obtidos para outra pessoa, podendo esta ser mal intencionada ou não.

Com base na Cartilha de Segurança Para Internet (2012, p.27):

> Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
> Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

> **Legítimo:** quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
> **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Do mesmo modo, ficaram evidenciadas todas as desvantagens causadas pela atuação dos spywares.

4.6 Keylogger e Screenlogger

Outras modalidades de programas maliciosos muito utilizados são os Keyloggers e os Screenloggers que são espécies de spyware e apresentam aspectos peculiares que merecem evidência.

O Keylogger grava todas as teclas que o usuário digita e usualmente, necessita de um ato anterior deste para que seja ativado, como por exemplo, entrar em um site de comércio eletrônico ou em um site de banco, atua capturando as senhas e outras informações que sejam de suma importância. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.27)

Assim sendo, este programa é extremamente perigoso, já que ele armazena tudo que a vítima digita no teclado do computador podendo inclusive descobrir senhas e outros dados sigilosos, ele não é instalado automaticamente, portanto necessita que o usuário entre em algum site que contenha um spyware para tanto.

Já o Screenlogger é uma forma mais evoluída do Keylogger, tendo em vista que este grava por meio de imagem a área em torno da posição em que o mouse é clicado ou a tela exibida no monitor de vídeo e a posição do cursor do mouse nos momentos em que este é clicado. Método muito utilizado por invasores para coletar as teclas digitadas pelos usuários em teclados virtuais que são disponibilizados especialmente em sites de bancos. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.27)

Deste modo, os modelos de teclados virtuais, utilizados pelos serviços bancários on-line, criados para evitar a coleta de senhas pelo keylogger, agora estão sujeitos à atuação do screenlogger que é uma versão mais moderna daquele e que captura a tela do computador.

Sendo evidentes os riscos que o computador corre se estiver sob o efeito destes programas invasores, já que senhas e outros dados sigilosos de extrema importância podem ser descobertos, causando enormes prejuízos para as suas vítimas.

Com os avanços da tecnologia, cada dia que passa são inventados novos meios de praticar delitos virtuais, não restando dúvidas de que todos esses programas invasores são formas de realizar tais delitos.

5 DAS CONDUTAS DELITUOSAS PRATICADAS NA INTERNET

As condutas delituosas praticadas na internet são aquelas que possuem o objetivo de lesar, roubar, ofender, infamar, realizar um abuso psicológico ou físico a outra pessoa. Essas condutas são concretizadas contra um indivíduo ou contra bens materiais e imateriais, estes comportamentos quando dizem respeito a bens podem ser relacionados a bens do governo, por exemplo, dos bancos ou bens de uma pessoa, no caso de roubo exemplificando.

Existem diversos tipos de crimes virtuais, merecendo destaque os crimes contra a honra, crimes contra a liberdade individual, crimes contra o patrimônio, crimes contra os costumes, crimes de invasões de privacidade e crimes de lesões a direitos humanos que serão mais bem analisados a seguir.

5.1 Crimes Contra a Honra

Os crimes contra honra sofreram um aumento considerável com a ampliação da internet e a chegada de novas ferramentas tecnológicas. Postar em uma rede social que um sujeito é criminoso, por exemplo, é uma prova indiscutível de calúnia, onde muitas pessoas acabam testemunhando o fato.

O principal motivo que leva os sujeitos ativos desses crimes a praticá-los é o fato de estes contarem com certo caráter anônimo e eles são praticados em sites, blogs, redes sociais, chats e e-mails, através do envio de spam, por meio de publicações, entre outras formas de postagens na internet.

Devido à facilidade em divulgar as informações e a rapidez com que estas se propagam neste meio, os crimes cometidos nele devem contar com o agravante de pena previsto no artigo 141, III do Código Penal. São delitos contra a honra: a calúnia, a difamação e a injúria.

Com base no artigo 138 do Código Penal, a calúnia consiste em uma declaração falsa e que desonre uma pessoa, mesmo que ela esteja morta. Ocorre

quando alguém de má-fé, utilizando de falsa alegação, imputa a um sujeito a prática de um crime.

De acordo com o artigo 139 do Código Penal, constitui difamação o ato de uma pessoa conferir a outra um fato que ofenda a reputação desta, ofendendo, portanto, a sua honra objetiva, este crime tem a sua consumação quando outro sujeito (terceiro) tem ciência do fato atribuído. Essa atribuição ofende a honra e a reputação de alguém e apresenta o objetivo de fazer com que este seja desacreditado perante a sociedade. A difamação atinge a moral do sujeito passivo.

Já a injúria, segundo o artigo 140 do Código Penal, consiste em um sujeito imputar a outro uma qualidade negativa, fazendo com que sua dignidade ou seu decoro seja ofendido. Trata-se de um crime que ocorre quando há uma ofensa de forma verbal, escrita ou física (injúria real) à dignidade ou ao decoro de uma pessoa, fazendo com que sua moral e seu ânimo sejam ofendidos.

Como não existe uma lei específica para punir estes crimes realizados na internet, eles são punidos pelos artigos do Código Penal Brasileiro de 1940, sendo o crime de calúnia previsto no artigo 138, a difamação no 139 e a injúria no 140 deste Código.

A principal alegação para que não haja uma lei específica para estes delitos é que as condutas praticadas pelo sujeito ativo são as mesmas das previstas no Código Penal, o que muda é o meio onde estes crimes são praticados, ou seja, na internet.

A polícia e os juízes apresentam muitas dificuldades para controlar e punir estes crimes ocorridos na internet, porque é muito complexo remover o conteúdo ofensivo deste meio e distinguir uma brincadeira de um crime.

5.2 Crimes Contra a Liberdade Individual

Os crimes contra a liberdade individual são divididos em crimes contra a liberdade pessoal, contra a inviolabilidade do domicílio, contra a inviolabilidade de correspondência e contra a inviolabilidade dos segredos.

As infrações contra a liberdade pessoal são: Constrangimento ilegal (artigo 146 do Código Penal), Ameaça (artigo 147 do Código Penal), Sequestro e cárcere privado (artigo 148 do Código Penal) e Redução a condição análoga à de escravo (artigo 149 do Código Penal).

Já os atos repreensíveis contra a inviolabilidade do domicílio são os de Violação de domicílio (artigo 150 do Código Penal).

As transgressões contra a inviolabilidade de correspondência são: Violação de correspondência (artigo 151 “caput” do Código Penal), Sonegação ou destruição de correspondência (§ 1º, I do artigo 151 do Código Penal), Violação de comunicação telegráfica, radioelétrica ou telefônica (§ 1º, II, III e IV, § 2º, § 3º e § 4º do artigo 151 do Código Penal) e Correspondência comercial (artigo 152 do Código Penal).

E por fim, as infrações criminais contra a inviolabilidade dos segredos são as de Divulgação de segredo (artigo 153 do Código Penal), Violação do segredo profissional (artigo 154 do Código Penal) e Invasão de dispositivo informático (artigo 154-A do Código Penal).

A violação de correspondência, divulgação de segredo e violação do segredo profissional se utilizam da equiparação dos documentos virtuais aos documentos tradicionais, porque não interessa qual é o meio de envio desses documentos, o que importa é que as informações foram violadas.

Mas nesses crimes contra a liberdade individual merece destaque o de invasão de dispositivo informático que foi criado pela lei 12.737 de 30 de Novembro de 2012, vale ressaltar que até então não existia uma lei para tipificar os delitos virtuais.

Conforme os artigos 154-A e B do Código Penal, as condutas tipificadas são:

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

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (GRIFO NOSSO)

Sendo assim, com o advento da lei 12.737/2012 trazendo a inclusão dos artigos 154-A e 154-B no Código Penal, as condutas de invadir dispositivo informático e produzir, oferecer, distribuir, vender ou difundir um dispositivo ou programa de computador com a finalidade de invasão do mesmo, enfim foram tipificadas, no capítulo seguinte será demonstrado se essa tipificação é suficiente para inibir a prática destes delitos.

5.3 Crimes Contra os Costumes

Os crimes contra os costumes são os de favorecimento à prostituição, de escrito ou objeto obsceno (artigo 234 do Código Penal), a pedofilia e tratam-se daqueles crimes que são contrários aos padrões ditados pela coletividade.

A pedofilia nada mais é do que a prática de atos libidinosos com menores de idade agindo contrariamente aos bons modos e contra a ingenuidade de quem ainda está em processo de formação tanto física quanto psicologicamente.

Quando os pedófilos realizam a exploração sexual dessas crianças, as transformando em uma mercadoria do sexo, esse crime é chamado de favorecimento a prostituição de menores de idade (artigo 218-B do Código Penal) e existe também, o crime de favorecimento a prostituição (artigo 228 do Código Penal), no qual é responsabilizado criminalmente quem induz ou atrai alguém para a prostituição, facilitando ou impedindo que a pessoa a abandone.

Existem diversos sites relacionados com a prostituição e a pornografia e é muito corriqueiro, ao navegar na internet, aparecerem sugestões de sites relacionados a esse conteúdo ou até mesmo a página que a pessoa está acessando ser redirecionada para outras de tais temas.

Conforme Liliane Pereira e Guilherme Gottardi (2014), uma prática muito comum no ambiente virtual ou pessoalmente é a chamada “Ficha Rosa” ou “Ficha Azul”, sendo que a rosa se refere às mulheres e a azul se refere aos homens, trata-se de modelos ou promotores de eventos que ao declararem fazer ficha rosa ou azul estão dizendo que aceitam fazer programa, tendo inclusive agenciamento de empresas para essa conduta. Importante ressaltar que quem apoia esse comportamento ao induzir ou atrair, facilitar ou impedir que alguém abandone esse exercício, estará praticando o crime de favorecimento a prostituição.

Levando-se em conta que as redes sociais são responsáveis por 80% dos casos de pedofilia no país, houve uma necessidade do legislador tipificar esse comportamento por meio da criação da lei 11.829 de 2008, que incluiu os seguintes artigos no ECA (Estatuto da Criança e do Adolescente):

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (GRIFO NOSSO)

Portanto, quem captura, reproduz, dirige ou produz, através de qualquer meio, cena de sexo explícito ou de pornografia que envolva menores de idade, assim como quem de qualquer forma intermedeia a participação de criança ou adolescente nestas cenas, pratica crime, sendo caso de aumento de pena o agente cometer o fato no exercício de cargo ou função pública, em razão de relações domésticas ou por possuir autoridade sobre as vítimas seja com o consentimento destas ou não.

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (GRIFO NOSSO)

Também pratica infração penal quem comercializa qualquer documento que tenha conteúdo sexual ou obsceno envolvendo quem está na infância ou na juventude.

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (GRIFO NOSSO)

Assim, quem de algum modo divulga, especialmente através da informática ou da telemática, um registro contendo conjunção carnal explícita ou obscenidades de meninos ou jovens, comete fato típico, bem como quem garante o armazenamento ou o acesso através da rede de computadores a esses registros, sendo que esses últimos, somente serão responsabilizados quando quem tem o dever legal de prestar serviço é notificado, mas não remove o conteúdo impróprio que está sendo espalhado.

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido. (GRIFO NOSSO)

Deste modo, é punível a conduta de quem obtém, possui ou guarda fotografia ou vídeo ou algum outro tipo de documento que apresente cena de sexo explícito ou pornográfica que envolva criança ou adolescente, a pena estipulada sofre diminuição quando o criminoso tem pouco material com ele.

Não realiza infração criminal quem tem a posse ou armazena este conteúdo com o objetivo de avisar às autoridades competentes, desde que seja agente público no exercício de suas funções, membro de instituição que possui o fim de avisar a respeito destes ilícitos ou representantes legais e funcionários de provedor de acesso a Internet e essas pessoas devem manter sigilo sobre o registro inadequado.

> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (GRIFO NOSSO)

Assim sendo, pratica transgressão quem simula de alguma maneira a participação de quem está na infância ou na juventude em eventos que tenham o teor sexual ou obsceno, também incorre em penalidade quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena este material.

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Nas mesmas penas incorre quem:
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. (GRIFO NOSSO)

E por fim, comete atos repreensíveis quem alicia, assedia, instiga ou constrange, através de um meio de comunicação, uma criança, sendo responsabilizado também, aquele que facilita de alguma forma o acesso do sujeito passivo ao conteúdo impróprio, ambas as condutas com a finalidade de fazer a vítima praticar ato libidinoso e quem apresenta qualquer comportamento entre estes citados com o objetivo de fazer o menor impúbere se expor pornográfica ou sexualmente.

> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (GRIFO NOSSO)

Portanto, fica evidenciado que devido ao elevado número de condutas criminosas de caráter sexual e obsceno praticadas contra a criança e o adolescente no ambiente cibernético, existiu uma necessidade por parte do legislador em tipificar tais comportamentos, com o intuito de inibir e culpar adequadamente os infratores.

5.4 Crimes Contra a Fé Pública

Fé Pública nada mais é do que confiar no caráter autêntico que a coletividade coloca em determinados documentos, sinais, atos, símbolos, entre outros, utilizados por todos no cotidiano, em virtude da importância probatória que o direito os confere.

Os crimes contra a Fé Pública estão divididos nos seguintes capítulos: Da Moeda Falsa (artigos 289/292 do Código Penal), Da Falsidade de Títulos e Outros Papéis Públicos (artigos 293/295 do Código Penal), Da Falsidade

Documental (artigos 296/305 do Código Penal), De Outras Falsidades (artigos 306/311 do Código Penal) e Das Fraudes em Certames de Interesse Público (artigo 311-A do Código Penal).

Desses delitos acima citados, merece destaque o previsto no artigo 298 do Código Penal, qual seja, o de falsificação de documento particular, que com o advento da lei 12.737 de 30 de novembro de 2012, obteve a inclusão de um parágrafo único para tipificar os atos de falsificação de cartão de crédito ou débito, equiparando estes ao documento particular previsto no caput do artigo.

5.5 Crimes de Lesões a Direitos Humanos

Os crimes de lesões a direitos humanos compreendem o terrorismo, ciberterrorismo no ambiente virtual, crimes de ódio, racismo, entre outros.

O ciberterrorismo é um exercício de terrorismo por meio da internet visando causar lesões a sistemas computacionais.

No dia 10 de novembro de 2009, dezoito estados do Brasil e boa parte do Paraguai ficaram sem energia por seis horas. Essa é só uma amostra do que pode acontecer em um país ao sofrer um ataque de criminosos virtuais. (SALVADORI, 2013)

Apesar do governo brasileiro não admitir, segundo o serviço de inteligência Norte Americano, o Brasil já sofreu ataques de ciberterroristas em dois momentos: em janeiro de 2005 quando o Rio de Janeiro lidou com quedas de luz e em setembro de 2007 quando três milhões de pessoas ficaram sem energia em Espírito Santo, sendo que a capital do estado teve lojas furtadas, hospitais em pane, celulares sem sinal e desordem no trânsito. (SALVADORI, 2013)

Os terroristas da internet normalmente atuam de forma bem organizada, combinando ataques através de grupos de conversas, fóruns virtuais e visam atingir quatro setores: bancário, de energia, de telecomunicação e de transporte, porque eles sabem que se alguma coisa ocorrer em um destes departamentos, o país inteiro sofrerá as consequências e esse crime é realizado por meio de um ataque virtual ou pela invasão de um sistema.

Muitos especialistas afirmam que a guerra do futuro será cibernética, tendo em vista que para os países, surtirá bem mais efeitos derrubar um sistema de uma nação do que matar pessoas.

Já os crimes de ódio, estão cada vez mais ganhando espaço nos ambientes virtuais, devido ao fato desse meio autorizar a conduta anônima e por transmitir a ideia de impunidade. As redes sociais apresentam diversos posicionamentos racistas, classistas, preconceituosos, de intolerância a religiões e até mesmo discriminações com portadores de necessidades especiais, entre outras formas.

Tais ilícitos merecem uma atenção especial ao serem praticados na internet, porque eles acabam influenciando outras pessoas a agirem da mesma forma, então, o que seria apenas um caso isolado de crime de ódio, acaba se tornando uma conduta discriminatória, preconceituosa e agressiva de um enorme grupo de pessoas.

Os crimes de racismo são caracterizados pelas atitudes discriminatórias sociais realizadas quando alguém julga as pessoas com base em seus aspectos religiosos, sexuais, econômicos ou físicos, especialmente quanto à cor da pele destas.

Esses crimes estão previsto no artigo 5º, XLII da Constituição Federal brasileira onde determina que a “prática do racismo constitui crime inafiançável e imprescritível, sujeitos à pena de reclusão, nos termos da lei”.

Se a conduta for uma injúria determinada por informações relacionadas com a raça, cor, etnia, religião, origem ou a condição da pessoa idosa ou portadora de deficiência, quem a praticou responderá pelo crime do artigo 140 § 3º do Código Penal, agora se não se tratar de injúria, o sujeito ativo irá responder pelos crimes previstos na lei anti-racismo (lei 7.716/1989) que tipifica os comportamentos discriminatórios ou preconceituosos quanto a raça, cor, etnia, religião ou procedência nacional.

Importante mencionar que a lei 12.735/12, popularmente conhecida como Lei Azeredo (em virtude de ter sido proposta pelo então senador Eduardo Azeredo), introduziu um novo artigo na lei de combate ao racismo (7.716/89) com o

objetivo de obrigar que publicações racistas sejam removidas de imediato da internet por meio de decisão judicial.

Deste modo, fica clara a intenção desta lei em evitar que postagens de cunho racista sejam constantemente disseminadas pela Internet, tendo em vista que tais condutas no ambiente cibernético acabam por influenciar outras pessoas a agirem da mesma forma.

6 DA DIFICULDADE DA REPRESSÃO AOS CRIMES VIRTUAIS

Muitos avanços ocorreram na repressão aos crimes virtuais nos últimos anos, merecendo mencionar o advento das leis 12.735/12, 12.737/12 e 12.965/14.

A lei 12.737/12 (Lei Carolina Dieckmann) tipificou as condutas de invadir dispositivos informáticos e conseguir ou modificar dados para obter vantagem indevida; produzir, oferecer ou vender programas maliciosos de computadores responsáveis pela invasão destes.

Outra conduta prevista na lei, obter através da invasão computacional informações confidenciais, segredos comerciais e infringir comunicações eletrônicas privadas; interromper ou perturbar serviço de internet e por fim, equiparar a falsificação de cartões de débito ou crédito aos crimes de falsificação de documento particular.

Com a criação da lei 12.735/12 (Lei Azeredo) foram incluídas as determinações de criar delegacias especializadas no combate de crimes informáticos tanto na polícia federal quanto nas polícias civis e de obrigar a retirada de publicações racistas de imediato da internet por meio de decisões judiciais, além da responsabilização pelo Código Penal Militar para quem entregar dados eletrônicos a um inimigo do Estado.

Já a lei 12.965/14 (Lei do Marco Civil da Internet), também conhecida como a constituição do uso da internet trouxe como principais novidades a neutralidade da rede (as operadoras somente podem vender pacotes de internet com a limitação da quantidade de dados que os usuários podem acessar e da velocidade de sua conexão).

A lei também trouxe o direito a privacidade na internet (o registro dos serviços proporcionados será guardado pelas operadoras no prazo de um ano e pelos sites no prazo de seis meses, esses dados são confidenciais e só serão fornecidos por pedido judicial) e a não responsabilização de um site por publicações de seus usuários (quando houver pedido judicial, ele tem a obrigação de remover o conteúdo, o site só será responsabilizado caso não cumpra com esta solicitação).

Apesar da problemática com a tipificação ter sido superada, os criminosos não se sentiram inibidos, tanto é que a Symantec (empresa que emprega suas funções na segurança da internet e das redes domésticas ou de companhias) juntamente com a OEA divulgaram um relatório em julho de 2014 que apontou o Brasil como o país da América Latina que mais gerou atividade maliciosa na internet.

Conforme esse relatório, o Brasil desembolsou US$ 8 bilhões (mais de R$ 18 bilhões) em estragos ocasionados pelos crimes virtuais. (DATA CENTER DYNAMICS-FOCUS, 2014)

Já na região de Presidente Prudente/SP, de acordo com o Departamento de Polícia Judiciária de São Paulo Interior, no ano de 2013 foram feitos 340 registros digitais de ocorrência, contra 229 registros somente no primeiro semestre de 2014. (JULIANI, 2014)

Os pontos que mais dificultam a repressão a esses delitos são a necessidade de profissionais atualizados; a dificuldade de identificação do autor desses ilícitos, bem como o aperfeiçoamento destes; a necessidade de mais órgãos investigativos no país; a precariedade das ferramentas investigativas, os questionamentos deixados pela lei 12.737/12 ter sido elaborada às pressas e os assuntos a respeito da competência dos crimes virtuais.

Deste modo, ainda existem diversos aspectos que necessitam de melhorias para o devido combate aos crimes de informática que serão estudados de forma mais aprofundada a seguir.

6.1 Necessidade de Aperfeiçoamento dos Profissionais

Os delitos de informática aumentaram de forma proporcional aos avanços tecnológicos, no entanto, a atuação estatal para punir adequadamente os agentes maliciosos, não acompanhou tal evolução.

Para que ocorra uma ação do Estado segura é necessário que constantemente os profissionais responsáveis pelo combate aos crimes virtuais se atualizem. Esses trabalhadores são os policiais, peritos criminais, legisladores, juízes e demais operadores do direito.

Uma das dificuldades mais encontradas para a devida punição dos agentes que praticam esses delitos é a ausência de capacitação dos peritos criminais para que possam descobrir quem é o sujeito ativo.

A prova pericial é a mais importante para determinar a materialidade do crime e a identificação do autor dele, sendo que o perito examina o dispositivo utilizado pela vítima da prática do ilícito penal para que descubra essas informações.

Levando-se em conta que os delinquentes agem, em sua maioria das vezes, sem deixar rastros, atuando de maneira silenciosa, os peritos criminais devem se atualizar sempre, porque os progressos na tecnologia e na informática são céleres e abundantes.

Com a constante modernização dos dispositivos que acessam a internet e com a popularização destes, as demandas existentes se tornaram bem distintas das que o legislador havia imaginado.

Os crimes cibernéticos surgiram no Brasil no final da década de 90 e somente em 2013 é que leis específicas para eles entraram em vigor, ficando evidente o atraso dos operadores do direito com relação a essas condutas criminosas.

Por isso, é preciso que o legislador esteja sempre atualizado para que novas leis sejam criadas conforme novas condutas sejam realizadas, contribuindo para que o direito possa acompanhar os avanços tecnológicos, bem como a evolução dos métodos utilizados para a prática de tais delitos.

Embora diversos comportamentos tenham sido tipificados nos últimos anos, a dificuldade de punição é atribuída à falta de capacitação por parte de diversos profissionais e não somente pela ausência de leis.

De acordo com o delegado Emerson Wendt, os papeis da polícia no ambiente cibernético são dois: “agir de modo a reprimir os delitos, investigando-os, e, também atuar constantemente no aspecto preventivo, orientando os usuários quanto ao melhor uso na internet, evitando que sejam vítimas de algum crime virtual”. (ROHR, 2011)

É preciso também, que os policiais aperfeiçoem as suas noções relacionadas com a informática, de modo que procurem métodos mais eficazes ao

investigar e combater os crimes informáticos, tendo em vista que a falta de qualificação por parte dos policiais tem sido a maior dificuldade encontrada para a investigação e o esclarecimento desses delitos.

As autoridades policiais do mundo todo, como por exemplo, o FBI, estão desenvolvendo os Cybercops, que são policiais especificamente e altamente treinados e com equipamentos adequados para realizar o combate dos delitos na rede.

O chefe da Divisão de Repressão a Crimes Cibernéticos da Polícia Federal, Adalton Martins, confessa que o país está atrasado quanto à punição dos delitos virtuais. Segundo Martins (2008) apud Santos e Fraga (2010, p. 48) “ou a gente se especializa nisso, nas unidades Policiais, na Polícia Federal e nas Polícias Civis que já estão trabalhando nesses crimes em alguns Estados, ou vamos perder a guerra”.

Para o delegado Wendt, “[...] a polícia precisa de mais treinamento e agentes policiais em investigação [...] Sentimos, também, falta de mais peritos formados na área, justamente para que possam comparecer e realizar o que chamamos de perícia online”. (ROHR, 2011)

Sendo assim, para solucionar esse problema é imprescindível que existam treinamentos constantes para as autoridades policiais investigarem de forma apropriada tais condutas e outra solução seria a implantação, nas delegacias comuns, de um grupo de profissionais especializados em investigar práticas realizadas no ambiente digital.

Conforme a maior parte dos doutrinadores, uma das problemáticas encontradas no julgamento desses crimes é a carência de noção técnica por parte de advogados e autoridades judiciárias.

De acordo com Rogerio Silva (2008), um exemplo disso ocorreu quando a Daniela Cicarelli (apresentadora de televisão) e seu namorado Tato Malzoni foram flagrados em cenas íntimas em uma praia e as filmagens foram divulgadas no site que compartilha vídeos, o Youtube. O desembargador do caso, Ênio Santarelli Zuliani, tomou uma medida equivocada, solicitando que o site fosse retirado do ar no Brasil.

Essa determinação prejudicou todos os brasileiros usuários da internet que ficaram três dias sem poder entrar no site. Sendo que se o desembargador estivesse atualizado, ele saberia que poderia solicitar a retirada do ar apenas do vídeo íntimo que causou constrangimento para as vítimas.

Portanto, conclui-se que devido ao fato de não ser mais necessário estar no mesmo lugar que a vítima para se praticar um delito e com os habituais avanços na tecnologia, o número de casos delituosos tem crescido consideravelmente, fazendo com que seja de suma importância uma atualização por parte dos operadores do direito, para que estes conheçam não somente o direito material, mas também, saibam lidar com essas condutas e instrumentos modernos, para que o interesse dos sujeitos passivos seja resguardado e garantido.

6.2 Dificuldade de Identificação e Aprimoramento Constante do Autor de um Crime Cibernético

Os agentes causadores dos crimes virtuais acarretam muitos danos com suas condutas de invasão de sistemas, roubos de dados e muitas outras.

Tratam-se de pessoas extremamente inteligentes, com uma imensa noção sobre informática, que usam de variados métodos para alcançar os bens dos sujeitos passivos.

Os criminosos de hoje usam ferramentas de alta tecnologia para ocasionar a destruição de dados, capturar informações confidenciais e extorquir autoridades e governos. (SANTOS E FRAGA, 2010, p. 8-9)

Diariamente crimes cibernéticos são praticados, já que muitos utilizadores da rede mundial de computadores não se protegem contra a atuação dos sujeitos ativos desses crimes, sendo imprescindível a implantação de proteção em seus dispositivos.

Houve uma mudança de comportamento por parte dos autores desses delitos, uma vez que há dez anos, eles procuravam demonstrar que o computador dos usuários estava infectado por determinado vírus, hoje, eles buscam sempre passar despercebidos, agindo de forma silenciosa, por isso há uma necessidade das

grandes companhias se unirem para desenvolverem meios eficazes de identificação desses sujeitos ativos.

Os crackers, conhecidos como os hackers do mal, estão tão evoluídos que são capazes de invadir sites de governos de qualquer país e implantar códigos mal intencionados neles e ainda pior, são capazes até de derrubar um avião, caso consigam invadir o sistema que controla o tráfego de aviões. (SALVADORI, 2013)

Além de estarem sempre atualizados, ainda auxiliam outras pessoas que manifestam a vontade de também se tornarem crackers e disponibilizam programas maliciosos na internet para serem baixados e usados na prática de delitos.

Uma prática muito comum desses agentes é se aproveitarem de temas do momento, como a constante inflação que o país está vivendo, para inventar páginas de internet falsas e spams cheios de programas mal intencionados. Tendo em vista que as redes sociais são alvos de habituais infecções, é preciso cautela por parte dos usuários com relação ao conteúdo que irão acessar.

Outro método bastante utilizado é a criação de antivírus falsos, quando a vítima executa esse programa, ela na verdade está desabilitando as proteções que já existem em seu computador, fazendo com que seus dados pessoais sejam furtados e integrando o aparelho em uma rede de bots, usada para tirar sites do ar.

A dificuldade de identificação dos criminosos ocorre devido à precariedade de dados obtidos no momento de rastreá-los.

As informações da internet são dotadas de velocidade e liberdade e são demonstradas em bits (a menor unidade de dados que pode ser guardado ou transmitido, utilizado na informática) estas podem ser tranquilamente modificadas por conhecedores de computação, fazendo com que a prova do crime e da autoria sejam fragilizadas ou até mesmo desapareçam.

“[...] a máquina deste suposto agente, não raro, pode estar sendo controlada por terceiros criminosos”. Demonstrando mais um problema ao tentar identificar um autor de delito virtual. (SANTOS e FRAGA, 2010, p. 58)

Mais uma questão problemática na identificação desses criminosos é a utilização de proxies (ferramentas que mascaram a identidade da pessoa,

escondendo o endereço do computador), por mais que as autoridades descubram de qual computador ou dispositivo foi realizada a conduta, será extremamente complicado descobrir quem estava utilizando tal aparelho na ocasião investigada.

O meio utilizado para identificar a pessoa que praticou um ilícito é através do IP (conjunto de protocolos que comunicam os computadores com a internet), no entanto, por meio dele somente é possível a identificação da máquina utilizada, fato que não prova a autoria do crime, apenas dá indícios dela e meros indícios não são suficientes para que alguém seja condenado.

Para que se consiga provar o autor desses delitos é necessário realizar uma perícia no computador usado pela vítima, esse ato de investigação é um processo muito lento.

E por fim, um fator que basicamente impossibilita a descoberta do autor de um crime na internet é se este usar um wifi (rede de internet sem fio) livre para praticar tal conduta, essa rede pode ser encontrada em faculdades e shoppings, por exemplo. Lan houses são muito empregadas para essa prática também, por não exigir nenhuma formalidade para seus usuários.

Sendo assim, fica evidenciada a imensa dificuldade que os profissionais possuem com relação a identificação dos delituosos virtuais e com o constante aprimoramento dos métodos utilizados por eles.

6.3 Insuficiência de Órgãos Investigativos no País e Precariedade das Ferramentas Investigativas

Um profissional competente e que tenha a sua disposição as ferramentas mais avançadas tecnologicamente contribuem para que a atuação estatal seja mais célere e eficaz.

Assim, os maiores obstáculos encontrados para a punição dos criminosos da internet são a precariedade das ferramentas investigativas dos órgãos governamentais e a insuficiência de organismos especializados na investigação de tais crimes.

As delegacias especializadas na repressão dos delitos de informática estão presentes nos seguintes estados: São Paulo, Rio de Janeiro, Espírito Santo, Minas Gerais, Paraná, Rio Grande do Sul, Distrito Federal, Goiás (a Delegacia Especializada em Investigação de Crimes Cibernéticos não está ativa, sendo usada a Gerência de Inteligência da Polícia Civil), Pará, Mato Grosso, Sergipe, Piauí, Tocantins, Maranhão, Pernambuco, Bahia e Rondônia.

Embora diversos distritos tenham sido criados, ainda há insuficiência de órgãos investigativos no país, tanto é que a Lei Azeredo determinou a criação de delegacias especializadas no combate aos crimes virtuais na polícia federal e nas polícias civis.

Há também uma necessidade dos órgãos estatais utilizarem ferramentas adequadas e modernas para a prevenção e análise dos crimes na internet.

> As provas dos crimes cibernéticos possuem um alto grau de volatilidade, ou seja, quando se está analisando um sitio que está no ar, operando na rede mundial de computadores, estes de uma hora para outra se “apagam”. Nesse sentido, a missão do serviço de perícias e crimes cibernéticos do Instituto Nacional de Criminalística da Polícia Federal tem tido como objetivo validar e preservar as provas dos crimes praticados com o uso do espaço cibernético. (SANTOS E FRAGA, 2010, p.44)

Assim sendo, fica evidenciada a gravidade das situações em que instrumentos apropriados não são utilizados para a investigação dos crimes cibernéticos, uma vez que as provas correm o risco de serem perdidas, não sendo mais possível punir os devidos culpados e nem sequer provar a existência de um comportamento ilícito.

“[...] quase todo crime cometido, no qual há um computador relacionado, se as provas digitais não forem coletadas adequadamente, sem as ferramentas técnicas apropriadas, podem ser invalidadas em possível litígio judicial”. (SANTOS E FRAGA, 2010, p.78).

O delegado Emerson Wendt, em entrevista concedida para o G1, discorreu a respeito dos mecanismos utilizados pelas autoridades policiais: “Utilizamos muitas ferramentas 'free' existentes e disponibilizadas para download e/ou

ferramentas virtuais, como aquelas que auxiliam na leitura de um código fonte de e-mail, por exemplo". (ROHR, 2011).

De acordo com Altieres Rohr (2011), essa mesma autoridade ainda respondeu ao questionamento sobre o que necessita melhorar para a devida punição dos crimes virtuais:

> Acho que precisa de mais treinamento e agentes policiais em investigação, além de equipamentos e ferramentas adequadas. [...] Acredito que para 2011 – se o planejamento dependesse só de mim – o ideal seria termos ao menos uma Delegacia de Polícia em cada Estado, interagindo e trabalhando em conjunto no combate aos crimes praticados no ambiente virtual.

Apesar de essa perspectiva ser do ano de 2011, nota-se que os aspectos que foram apontados como fragilizados, ainda permanecem, exemplificando, ainda não temos uma delegacia especializada na investigação e repressão aos delitos informáticos para cada estado do país.

Deste modo, é preciso que mais delegacias sejam criadas, assim como, há uma necessidade de modernização dos mecanismos utilizados pelos profissionais que punem os crimes na internet, de modo que o país possa acompanhar a constante evolução destes e dos métodos utilizados para sua prática.

6.4 As Críticas Negativas Sobre a Lei 12.737 de 2012

Levando-se em conta que esta lei 12.737/12, também conhecida como Lei Carolina Dieckmann, foi sancionada às pressas, devido à pressão do povo e especialmente da mídia, já que uma atriz global teve suas fotos íntimas furtadas de seu computador e foi chantageada para que tais fotos não fossem publicadas na rede, muitas questões problemáticas surgiram desse advento apressado da lei.

Um dos pontos mais controversos dessa lei está previsto no "caput" do artigo 154-A do Código Penal:

> Art. 154-A. **Invadir dispositivo informático** alheio, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de **obter**, adulterar ou destruir dados ou

> informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (GRIFO NOSSO)

A polêmica maior está em torno da expressão “mediante violação indevida de mecanismo de segurança”, além de outras terminologias imprecisas que ocasionaram lacunas legislativas.

Se uma pessoa não tiver um antivírus e o seu dispositivo for invadido, existirá crime? Se o smartphone não apresentar uma senha de desbloqueio e furtarem informações dele, é crime? E se a alguém fornecer a senha do seu dispositivo para uma pessoa e esta vier a praticar um crime se aproveitando da situação, também não há crime?

Sendo assim, as pessoas que não apresentam conhecimentos técnicos e não protegem o seu dispositivo ou que não têm dinheiro suficiente para comprar programas de proteção, não poderiam se tornar vítimas de tal crime.

Desse modo, fica evidente que o princípio da igualdade está sendo ferido neste artigo, tendo em vista que não pode haver distinção entre os aparelhos que possuem ou não senha, todos devem ser protegidos pela lei.

A utilização do termo “invadir” pode contribuir para que muitos agentes fiquem sem punição caso estes não usem de violência para conseguir acessar os conteúdos dos aparelhos.

De acordo com Luiz Augusto Sartori de Castro (2012):

> O que colocamos em xeque é a produção de lei motivada pela casuística — aqui, o caso da atriz Carolina Dieckmann — e que, por assim ser, peca e muito na qualidade técnica de sua redação. Como exemplo, vale mencionar o verbo nuclear da proposta ao artigo 154-A, qual seja: “invadir”. Segundo o dicionário Aurélio, o verbo “invadir” significa “entrar à força, apoderar-se violentamente”. Assim, a subsistir a redação do novel artigo 154-A, somente se poderia cogitar da ocorrência de crime se, e somente se, o agente acessasse o dispositivo de informática à força, violentamente, em especial porque, em matéria de Direito Penal, a interpretação deve sempre ser restritiva. Ocorre que a prática desses atos atentatórios que o artigo 154-A visa a coibir, por excelência, nunca — ou quase nunca — ocorre unilateralmente, isto é, com o agente mal-intencionado tendo agido sozinho para acessar o sistema operacional. É que existem somente dois meios de acessar o banco de dados de um computador de modo indevido: 1) acessando fisicamente o próprio computador — o que é óbvio não se enquadra do tipo penal sob exame; ou 2) quando o usuário permite inadvertidamente que sejam instalados em seu computador os chamados malwares, que estão sorrateiramente ocultos em arquivos enviados por e-mails, em determinados links de

> internet ou em dispositivos móveis como pendrives. Ou seja, em nenhum de acesso remoto se pode dizer que o agente mal-intencionado agiu de modo violento para obter os dados do usuário. O que houve foi o emprego de ardil. Para resumir o que se sucede nesses casos, acaba sendo o próprio usuário a permitir que seus dados sejam acessados.
> [...] Mas nem tudo estaria perdido se o verbo "invadir" fosse substituído por "acessar".

Assim, o verbo "invadir" significa entrar à força, apoderar-se de forma violenta, então somente existiria crime se o sujeito ativo usasse de violência para acessar ao conteúdo do dispositivo, entretanto, essa situação quase nunca ocorre, porque as formas indevidas de acesso a um computador são utilizando ele de forma física, o que não é o caso desse artigo.

E usando os programas invasores que enganam suas vítimas, fazendo com que estas possibilitem a entrada de arquivos maliciosos em seus aparelhos sem ter o conhecimento disto, ficando claro que não houve o uso de violência nessas condutas, de forma que a solução seria substituir o presente verbo pelo de "acessar".

Outra terminologia criticada é a de "dispositivo informático", porque não somente eles acessam a internet na atualidade, temos as geladeiras, relógios, televisões que também entram na internet. Assim, o legislador deu a entender que caso esses aparelhos sejam invadidos, não serão protegidos por tal artigo.

Se um smartphone que apresenta bloqueio de tela automático e o seu dono o deixa em cima de uma mesa, antes de bloquear sozinho alguém mal intencionado pega o celular e furta as fotos, a dúvida que tem surgido é se tal ato configura crime.

Há também uma divergência doutrinária com relação ao fato do agente entrar no dispositivo de alguém apenas para espiar, existem entendimentos no sentido de que essa conduta é considerada como o verbo "obter" previsto no artigo e entendimentos de que tal comportamento não configura crime algum.

Importante mencionar que alguns aspectos favorecem a ineficácia dessa lei, sendo eles as penas brandas que possibilitam a conversão das penas restritivas de liberdade em penas restritivas de direitos e a rápida prescrição que torna difícil a tarefa de punir o agente.

As penas para esses delitos são de três meses a um ano, ou seja, são completamente desproporcionais aos comportamentos delituosos, além de serem

incapazes de inibir a atuação do infrator, fazendo com que os agentes sejam submetidos aos institutos despenalizadores do Juizado Especial Criminal, como a transação penal e a suspensão condicional do processo, por exemplo.

Essas brechas legislativas contribuem para que os transgressores utilizem os duplos sentidos em suas teses defensivas para se isentarem de punição.

Esses delitos, devido a sua complexidade, são incompatíveis com o rito sumaríssimo do Jecrim, uma vez que para provar a autoria é necessária a produção de prova pericial, que é complexa e demanda certo tempo.

A ausência de preparo dos policiais ao investigar tais crimes pode contribuir para que estes prescrevam.

Muito embora existam delegacias especializadas em vários estados brasileiros, estas não são suficientes para conter a elevada quantidade de crimes desta espécie, bem como apresentam policiais despreparados que contribuem para o retardamento da investigação. O problema é que as penas atribuídas para as condutas criminosas são bem leves e consequentemente, a prescrição é rápida, caso as autoridades policiais demorem muito em sua atuação, o crime estará prescrito antes que termine de agir.

Portanto, apesar desta lei significar um avanço no ordenamento jurídico brasileiro, é evidente a necessidade de leis complementares e de jurisprudências para que esta lei seja eficaz, de modo que as lacunas legislativas, ambiguidades e falhas sejam superadas.

6.5 A Competência dos Crimes Virtuais

Uma das maiores situações problemáticas quanto aos crimes virtuais é o conflito de competência, tendo em vista que a Internet possibilita que o sujeito ativo esteja em qualquer lugar do mundo e que o sujeito passivo seja brasileiro.

Importante ressaltar que o Brasil adota o Princípio da Territorialidade, sendo assim, se o delito for praticado dentro do país, independentemente do autor e da vítima serem brasileiros, essa infração penal será punida pela legislação brasileira.

O crime praticado no Brasil será de competência federal nos casos previstos no artigo 109 da Constituição Federal Brasileira, se o ilícito penal não se encaixar nas hipóteses taxativas dessa norma, a competência será estadual, ou seja, a competência estadual é subsidiária.

Se for feita uma interpretação restritiva do artigo 109 da Constituição Federal, não será encontrado nenhum inciso tratando dos delitos de informática. Portanto, conforme o inciso IV dessa norma, somente será competência federal aqueles delitos cometidos contra o Estado, empresas estatais ou suas autarquias.

Deste modo, a competência do crime será determinada pelo artigo 69 do Código de Processo Penal:

> Artigo 69 – Determinará a competência jurisdicional:
> I – o lugar da infração;
> II – o domicílio ou residência do réu;
> III – a natureza da infração;
> IV – a distribuição;
> V – a conexão ou continência;
> VI – a prevenção;
> VII – a prerrogativa de função.

Sendo que essa competência jurisdicional é referente a jurisdição comum que engloba as federais e estaduais.

Esse é um ponto com bastante contradição, levando em conta que até mesmo os julgados nos tribunais não são pacíficos:

> PORNOGRAFIA INFANTIL – JUSTIÇA FEDERAL.
> CONFLITO NEGATIVO DE COMPETÊNCIA. DIVULGAÇÃO DE IMAGENS PORNOGRÁFICAS DE MENORES POR MEIO DA INTERNET. CONDUTA QUE SE AJUSTA ÀS HIPÓTESES PREVISTAS NO ROL TAXATIVO DO ART. 109 DA CF. COMPETÊNCIA DA JUSTIÇA FEDERAL. **CC 120999/CE, Rel. Ministra ALDERITA RAMOS DE OLIVEIRA (DESEMBARGADORA CONVOCADA DO TJ/PE), TERCEIRA SEÇÃO, julgado em 24/10/2012, DJe 31/10/2012.**
>
> Troca de mensagens com pornografia infantil – Justiça Estadual.
> CONFLITO DE COMPETÊNCIA. CRIMES RELACIONADOS À DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO ENVOLVENDO CRIANÇAS E ADOLESCENTES POR MEIO DA INTERNET. INEXISTÊNCIA DE ELEMENTOS DE INTERNACIONALIDADE. COMPETÊNCIA DA JUSTIÇA ESTADUAL. PRECEDENTES DO STJ. **CC 121215/PR, Rel. Ministra ALDERITA RAMOS DE OLIVEIRA (DESEMBARGADORA CONVOCADA DO TJ/PE), TERCEIRA SEÇÃO, julgado em 12/12/2012, DJe 01/02/2013).**

Outra questão problemática acontece quando o delito é internacional. Levando-se em consideração que o Brasil adota o princípio geral da territorialidade, suas leis se limitam ao território brasileiro, portanto, não são aplicadas no exterior. Sendo assim, quando o delito for internacional, será submetido a competências extraordinárias extraterritoriais.

Corroborando esse entendimento Sergio Marques Roque (2007, p. 60-61):

> [...] a questão que suscita maiores dúvidas é a dos crimes que a distanciam como nos casos dos delitos praticados através da Internet quando a ação é executada em um país e seus efeitos ocorrem no Brasil.
> Como resolver, então, este problema? A solução estaria na celebração de tratados internacionais. Mas para isso ser possível há necessidade da existência, primeiramente, da dupla incriminação, ou seja, que as condutas constituam crime em ambos os países.
> Outra questão que se coloca é a extradição, pois como o Brasil não concede a extradição a um seu cidadão para ser processado em um outro pais, haverá reciprocidade no caso da ação ter sido praticada em território estrangeiro por cidadão não brasileiro.

A respeito do Direito Internacional Público, quando um delito é praticado por estrangeiro que esteja no Brasil, pode ocorrer a extradição, porém é necessário que alguns requisitos sejam preenchidos, exemplificando: é preciso que exista uma celebração de Tratado ou Convenção entre ambos os países e que verse sobre as extradições, sendo competente a justiça que solicitou a extradição.

Também é necessário que exista uma dupla incriminação, ou seja, o crime praticado deve ser tipificado em ambos os países, tanto no solicitante quanto no solicitado; caso haja pena de morte, é preciso que ocorra a comutação desta pena, devendo ser comutada até 30 anos, conforme a legislação brasileira, cuja punição máxima seria de 30 anos de pena privativa de liberdade.

Outros requisitos que merecem destaque: o acusado que seja submetido à extradição não pode ser sujeito a tribunal ou juiz de exceção; o delito deverá possuir certa gravidade, caso não possua, o infrator não será extraditado; não será extraditado aquele que cometer ato ilícito considerado contravenção e a competência do procedimento de extradição é do Supremo Tribunal Federal.

E por fim, outra questão problemática ocorre quando um delito é praticado por brasileiro nato e a vítima é estrangeira, sendo necessária a extradição do brasileiro

nato. Neste caso, leva-se em consideração a previsão do artigo 5º, LI da Constituição Federal:

> **Art. 5º -** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> **LI** - nenhum brasileiro será extraditado, salvo o naturalizado, em caso de crime comum, praticado antes da naturalização, ou de comprovado envolvimento em tráfico ilícito de entorpecentes e drogas afins, na forma da lei;

Assim, nenhum brasileiro que pratique um delito cibernético será extraditado, fato que gera uma intranquilidade em relação aos atos ilícitos que ultrapassam as barreiras territoriais do Brasil. Ficando evidente que essa lacuna precisa ser resolvida, tendo em vista que para os delitos de informática não existem fronteiras.

7 CONCLUSÃO

Dos estudos efetuados e acima expostos, conclui-se que apesar de diversos avanços terem acontecido com a criação das leis 12.735/12, 12.737/12 e 12.965/14 (Lei do Marco Civil da Internet) tipificando condutas delitivas na internet e garantindo direitos para os usuários, as dificuldades quanto à repressão dos delitos de informática ainda persistem.

Os problemas ocorrem devido à necessidade de aperfeiçoamento dos profissionais, a dificuldade de identificação e o constante aprimoramento dos criminosos, a insuficiência de órgãos investigativos no país e a precariedade das ferramentas investigativas, os pontos controversos da lei 12.737/12 e as questões a respeito da competência dos delitos de informática.

Deste modo, há uma necessidade de atualização por parte dos profissionais responsáveis pela investigação, prevenção e repressão destes delitos; de um maior investimento em ferramentas adequadas e modernas para que os sujeitos ativos dessas infrações sejam identificados.

Também é preciso que mais órgãos investigativos sejam criados no país com profissionais devidamente capacitados e atualizados, para que a atuação estatal seja eficiente ao atender a elevada demanda dessas infrações; sejam criadas leis complementares e jurisprudências com o intuito de solucionar as omissões, ambiguidades e falhas da lei 12.737/12 e que os conflitos de competência dos delitos de informática sejam resolvidos.

Por fim, podemos concluir que apesar de resultados positivos terem sido alcançados nos últimos anos, o país ainda necessita melhorar em diversos aspectos para que a repressão aos crimes virtuais seja feita de forma eficiente possibilitando assim, que os profissionais responsáveis pela prevenção, investigação e combate aos delitos de informática possam acompanhar os avanços tecnológicos, bem como os constantes aperfeiçoamentos dos criminosos e dos métodos utilizados por eles.

REFERÊNCIAS

ANDRADE, Wesley Almeida. **Crimes na Internet: uma Realidade na Sociedade de Informação.** 2006. 57 f. Monografia (Bacharelado em Direito) – Faculdades Integradas “Antônio Eufrásio de Toledo”, Presidente Prudente, 2006.

BRASIL. Lei 7.716, de 05 de Janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 05 de jan. 1989. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em 08 nov. 2014.

BRASIL. Lei 11.829, de 25 de Novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 25 de nov. 2008. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em 10 nov. 2014.

BRASIL, Lei nº 12.735, de 30 de Novembro de 2012. Altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 05 de janeiro de 1989. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 30 de nov. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em 01 nov. 2014.

BRASIL. Lei nº 12.737, de 30 de Novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto- Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 30 de nov. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 10 nov. 2014.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 23 de abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 04 fev. 2015.

BRASIL. **Vade Mecum**/ **Código Penal.** 20 ed. atualizada e ampliada. São Paulo: Saraiva, 2015.

BRASIL. **Vade Mecum/ Código de Processo Penal.** 20 ed. atualizada e ampliada. São Paulo: Saraiva, 2015.

BRASIL. **Vade Mecum/ Constituição da República Federativa do Brasil.** 20 ed. atualizada e ampliada. São Paulo: Saraiva, 2015.

BRAZ, Talita Solyon. **Direito à Intimidade X Internet.** 2007. 52 f. Monografia (Bacharelado em Direito) - Faculdades Integradas "Antônio Eufrásio de Toledo", Presidente Prudente, 2007.

CARDOSO, Marcel dos Santos. **Crimes Virtuais e suas Peculiaridades.** 2008. 55 f. Monografia (Bacharelado em Direito) – Faculdades Integradas "Antônio Eufrásio de Toledo", Presidente Prudente, 2008.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** 2ª ed. Rio de Janeiro: Editora Lumen Juris, 2003.

CASTRO, Luiz Augusto Sartori de. "Lei Carolina Dieckmann" Seria a Salvação da Internet?. **Migalhas,** 21 nov. 2012. Disponível em: < http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet>. Acesso em: 22 abr. 2015.

COELHO, Ana Carolina Assis. **Crimes Virtuais: Análise da Prova.** 2008. 48 f. Monografia (Bacharelado em Direito) – Faculdades Integradas "Antônio Eufrásio de Toledo", Presidente Prudente, 2008.

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

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

DATA CENTER DYNAMICS. OEA e Symantec Apresentam Relatório Sobre Cibersegurança na América Latina. **Data Center Dynamics**, 04 jun. 2014. Disponível em: < http://www.datacenterdynamics.com.br/focus/archive/2014/06/oea-e-symantec-apresentam-relat%C3%B3rio-sobre-ciberseguran%C3%A7a-na-am%C3%A9rica-latina>. Acesso em 10 jul. 2014.

FASSINA, Ricardo. **Aspectos Criminais Sobre a Conduta do Hacker.** 2001.69 f. Monografia (Bacharelado em Direito) – Faculdades Integradas “Antônio Eufrásio de Toledo”, Presidente Prudente, 2001.

FELICIANO, Guilherme Guimarães. **Informática e Criminalidade (primeiras linhas).** Ribeirão Preto, SP: Nacional de Direito Livraria Editora, 2001.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital.** São Paulo: Saraiva, 2013.

JULIANI, Arize. Crimes Virtuais Somam 229 Ocorrências na Região. **O Imparcial**, 24 ago. 2014. Disponível em: < http://www.imparcial.com.br/site/crimes-virtuais-somam-229-ocorrencias-na-regiao>. Acesso em 12 nov. 2014.

KAMINSKI, Omar. **Internet Legal: O Direito na Tecnologia da Informação : Doutrina e Jurisprudência.** 1ª ed. (ano 2003), 5ª reimpr. Curitiba: Juruá, 2009.

LEONARDI, Marcel. **Tutela e Privacidade na Internet.** São Paulo: Saraiva, 2012.

MACEDO, Viviane Poiato. **Da Responsabilidade dos Hackers e Crackers no Direito Penal.** 2004. 55 f. Monografia (Bacharelado em Direito) – Faculdades Integradas “Antônio Eufrásio de Toledo”, Presidente Prudente, 2004.

MARQUES, Jader; SILVA, Maurício Faria da. **O Direito na Era Digital.** Porto Alegre: Livraria do Advogado Editora, 2012.

NOGUEIRA, Sandro D’ Amato. **Crimes de Informática.** 1ª ed. Leme/SP: BH Editora, 2008.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil.** São Paulo: Editora Atlas, 2000.

PEREIRA, Liliane; GOTTARDI, Guilherme. O Mercado da Ficha Rosa. **Jornalismo Econômico** / **Manhã**, 21 nov. 2014. Disponível em: <http://jornalismoeconomico.uniritter.edu.br/?p=425>. Acesso em 01 fev. 2015.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** 1 ª ed. (ano 2003), 4ª tir. Curitiba: Juruá, 2006.

ROHR, Altieres. Trabalho Contra Crimes Virtuais Ainda Está Longe do Ideal, Diz Delegado. **G1-Tecnologia**, 06 jan. 2011. Disponível em: < http://g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html>. Acesso em 10 fev. 2015.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual.** Belo Horizonte: Del Rey Editora, 2005.

ROQUE, Sérgio Marcos. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de Informática.** 1. ed. Campinas: Bookseller, 2002.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004.

SALVADORI, Fausto. Crimes Virtuais. **Revista Galileu**, 2013. Disponível em: < http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html>. Acesso em 05 abr. 2014.

SANTOS, Antonio Jeová. **Dano Moral na Internet.** São Paulo: Método, 2001.

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico.** São Paulo: OAB SP, 2010.

SANTOS, Fernando da Cruz Alves. **Aspectos Relevantes da Criminalidade Através da Informática.** 2003. 59 f. Monografia (Bacharelado em Direito) – Faculdades Integradas “Antônio Eufrásio de Toledo”, Presidente Prudente, 2003.

SÃO PAULO. Núcleo de Informação e Coordenação do Ponto BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Comitê Gestor da Internet no Brasil. **Cartilha de Segurança Para a Internet.** São Paulo, 2012. 126 p.

SILVA, Mauro Marcelo de Lima e. Crimes da Era Digital. Mauro Marcelo Diz Que Cenário do Crime na Internet é Desesperador. **Consultor Jurídico – Conjur,** 01 set. 2000. Disponível em: <http://www.conjur.com.br/2000-set-1/especialista_analisa_cenario_delitos_internet>. Acesso em 04 fev. 2014.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático: Problemas Fundamentais.** 2002. 146 f. Dissertação (Mestrado em Direito) – Universidade Estadual de Maringá, Maringá, 2002.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático.** São Paulo: Editora Revista dos Tribunais, 2003.

SILVA, Rogerio. O Efeito Cicarelli. **STOA – Universidade De São Paulo**, 01 out. 2008. Disponível em: < https://social.stoa.usp.br/rogeriosilva/blog/div-xmlns-http-www.w3.org1999xhtml-lang-pt-dir-ltr-o-efeito-cicarellidiv-33351>. Acesso em 10 abr. 2015.

TAKUSHI, Tiago Tadashi. **Crimes Virtuais: Aspectos Gerais, Persecução Criminal e de Competência.** 2009. 72 f. Monografia (Bacharelado em Direito) – Faculdades Integradas "Antônio Eufrásio de Toledo", Presidente Prudente, 2009.

TEIXEIRA, Tarcisio. **Direito Eletrônico.** São Paulo: Editora Juarez de Oliveira, 2007.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático: Do Acesso Não Autorizado a Sistemas Computacionais.** Rio de Janeiro: Editora Forense, 2003.