FACULDADES INTEGRADAS

“ANTÔNIO EUFRÁSIO DE TOLEDO”

CURSO DE PÓS-GRADUAÇÃO "LATO-SENSU"
DIREITO PENAL E PROCESSO PENAL

DOS CRIMES VIRTUAIS

CLÉBIO WILIAN JACINTHO

Presidente Prudente-SP

2.014

FACULDADES INTEGRADAS

“ANTÔNIO EUFRÁSIO DE TOLEDO”

CURSO DE PÓS-GRADUAÇÃO "LATO-SENSU"
DIREITO PENAL E PROCESSO PENAL

DOS CRIMES VIRTUAIS

CLÉBIO WILIAN JACINTHO

Monografia apresentada como requisito parcial para Conclusão da Especialização lato sensu em Direito Penal e Processo Penal, sob a orientação do Professor Marcus Vinicius Feltrim Aquotti.

Presidente Prudente-SP

2.014

DOS CRIMES VIRTUAIS

Monografia/TC aprovado como requisito parcial para obtenção do Grau de Especialista.

_____

Marcus Vinicius Feltrim Aquotti

Orientador

_____

Examinador 1

_____

Examinador 2

Presidente Prudente, 07 de Fevereiro de 2.014

"As nuvens mudam sempre de posição, mas são sempre nuvens no céu. Assim devemos ser todo dia, mutantes, porém, leais com o que pensamos e sonhamos; lembre-se, tudo se desmancha no ar, menos os pensamentos. "

Paulo Baleki

Dedico este trabalho à minha família, à minha namorada Daiane, aos meus amigos e colegas que me apoiaram nesta jornada.

AGRADECIMENTOS

Primeiramente, agradeço a DEUS.

Agradeço a minha família pelo apoio e dedicação que me foram depositados, bem como aos meus amigos e em especial à minha namorada Daiane pelo incentivo incondicional.

Ao meu orientador Marcus Vinicius Feltrim Aquotti, pelo incentivo, apoio e atenção dispensada no auxílio às atividades e discussões acerca do andamento desta Monografia de Conclusão de Curso.

Por derradeiro, porém, não menos importante, agradeço a todos os docentes pelo dom da didática e por nos fornecer tantas informações úteis e necessárias a esta especialização e à vida.

RESUMO

O objeto a que se destina essa Monografia é apresentar, e também informar, que os crimes virtuais estão se disseminando de uma forma nunca antes constatada, e que os Estados tem o dever de criar ferramentas precisas para impedir a prática de tais ilícitos. Que pessoas, por vezes desavisadas ou mesmo que não acompanharam a evolução tecnológica, estão sendo vítimas de criminosos “virtuais”, cujos quais se “escondem” na intrínseca malha virtual da rede. Há que se destacar a criação e aprovação de leis específicas, a exemplo da Lei nº 12.737/2.012, que dispõe sobre a tipificação criminal de delitos informáticos, referentes ao assunto que estão eclodindo em nosso país que, por muitos anos, ficou à margem desse tipo de legislação. Não podendo deixar de falar também num dos mais importantes projetos de lei que está prestes a ser aprovado, o Marco Civil da Internet, que certamente, irá revolucionar a forma como o serviço é prestado e utilizado. Por derradeiro, porém, não menos importante, há que se salientar que, apesar das leis e dispositivos legais à espécie, todo usuário precisa tomar as devidas precauções de segurança quando entra em contato com a rede mundial de computadores, pois, a exemplo de sua vida real, não devemos baixar a guarda, nem admitir a presença de pessoas ou mesmo hipóteses não confiáveis para não sermos vítimas dos famigerados crimes virtuais.

Palavras-chave: Crimes Virtuais. Criminosos Virtuais. Evolução Tecnológica. Ilícitos. Internet. Lei nº 12.737 de 2012. Malha Virtual. Marco Civil da Internet. Rede. Rede Mundial de Computadores. Usuário.

ABSTRACT

The object of the intended design of this monograph is to present and also inform that cybercrimes are spreading like never before observed, and that states have a duty to create accurate tools to prevent the commission of such crimes. That people sometimes or even unaware that did not follow the technological developments being victims of "virtual" criminals, whose which "hide" the intrinsic virtual mesh network. It is worth emphasizing the creation and adoption of specific laws, like the Law 12.737/2.012, which provides for the classification of computer criminal offenses pertaining to the subject that are hatching in our country that, for many years, was left out of this type of legislation. Can not fail to also speak one of the most important bills that are about to be approved, the Marco Civil Internet, which will certainly revolutionize the way the service is provided and used. For the last, but not least, it should be noted that, despite laws and legal devices to the species, every user needs to take the proper safety precautions when coming in contact with the world wide web, because, like his real life, we should not lower our guard, nor admit the presence of people or even unreliable assumptions not to be victims of the notorious cybercrimes.

Keywords: Virtual Crimes. Virtual Criminals. Technological Evolution. Unlawful. Internet. Law No. 12.737 of 2012. Virtual Grid. Civil Marco Internet. Network. World Wide Web. User.

LISTA DE ABREVIATURAS E SIGLAS

ADPF - Arguição de Descumprimento de Preceito Fundamental

CRACKER - Termo usualmente utilizado para designar quem pratica a quebra (ou cracking) de um sistema de segurança

COOKIE - Grupo de dados trocados entre o navegador e o servidor de páginas eletrônicas, colocado num arquivo (ficheiro) de texto criado no computador do utilizador

DEEP WEB – Termo utilizado para designar o submundo da internet

ECA – Estatuto da Criança e do Adolescente

E-COMMERCE – Comércio realizado por meio virtual/eletrônico

HACKER – São indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas

HARD DISK – Disco interno do computador, aonde se gravam e armazenam todos os tipos de informações

NCP - Network Control Protocol (Controle de Protocolo da Rede)

PASSWORD - Senha

SITE – (sítio) Endereço eletrônico comumente utilizado na internet

SPAM – Termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas

STF – Supremo Tribunal Federal

STJ – Supremo Tribunal de Justiça

TCP/IP - Transmission Control Protocol/Internet Protocol (Transmissão do Protocolo de Controle/Protocolo da Internet)

WWW - World Wide Web

SUMÁRIO

1 INTRODUÇÃO

A presente monografia analisou o desenvolvimento e a criminalização do mundo cibernético, seu surgimento, casos atuais, as leis e, em especial, sua atuação no Brasil, com a análise dos principais crimes e leis e, quanto à conclusão, fez uma análise mais abalizada no tocante ao futuro dessa nova modalidade de atuação.

O intuito de se escolher tal tema se dá pela constante e rápida evolução que existe nessa área e, em especial, pela crescente onda de ilícitos provenientes do mundo cibernético. Com isso, os direitos em concreto são atingidos, criando, no espaço virtual, uma “oportunidade” real para os fora da lei.

Tais práticas delituosas podem ocorrer das mais variadas formas, desde os tradicionais furtos e roubos, passando pela extorsão, dentre outras formas comuns de ilícitos, podendo alcançar novas formas, como o cyberbulling, que são igualmente nefastas e prejudiciais aos envolvidos.

O assunto em tela tem a sua importância na medida em que tais crimes estão apenas em seu nascedouro, ou seja, são embriões de outros mais perigosos e devastadores que estão por vir. A atividade da informática, não podemos deixar de admitir, esta incutida nas principais áreas dos setores cruciais de todo o mundo. A pergunta antes feita por centros de pesquisas aos entrevistados era: “Quantas horas por dia você passa conectado na internet?” hoje deve ser readequada para “Quantas horas por dia você não passa conectado na internet?”, pois todos estamos “on-line” diuturnamente, o que nós traz momentos úteis e importantes, porém, também vários inconvenientes e infortúnios, como por exemplo falhas na conexão ou, de uma forma mais grave, sermos vítimas de crimes virtuais.

Sabedor de todo o ocorrido, porém, menos ágil e rápido que o mundo tecnológico, o Governo Nacional tenta editar leis para frear essa onda que já dura há muito tempo, porém, a cada passo legal dado, tantos outros são dados ilegalmente pelos ciber infratores, o que torna as leis, em seu berço, já obsoletas e ineficazes.

Nota-se a existência de amplo posicionamento doutrinário e

jurisprudencial que, apesar de serem considerados recentes, já indicam um norte bastante concreto do que poderá ocorrer em breve.

Nota-se que as leis que estão sendo editadas e as já aprovadas, se preocupam, de uma forma bastante inteligente, com o cyberbulling e as invasões de privacidade, que atormentam os usuários da rede mundial de computadores.

Há que lembrar, também, que está em plena discussão, prestes a ser aprovado, o Marco Civil da Internet, projeto que, quando em execução, irá delimitar exatamente os direitos e deveres dos provedores e dos usuários da rede.

No tocante à metodologia, a mais amplamente utilizada no referido trabalho foi a denominada histórica, através da qual se pôde verificar a evolução digital no nosso Estado, bem como em todo o mundo. Outrossim, foram feitas pesquisas em jurisprudências, doutrinas, livros e sítios especializados, bem como em casos concretos atuais.

Por derradeiro, o trabalho em tela propõe uma conclusão no sentido de aferir se tais normas legais aplicáveis aos casos concretos são eficazes no sentido de se coibir a prática virtual delituosa.

2 A HISTÓRIA DA INTERNET

A internet, como a conhecemos hoje, deve-se, como a muitos outros inventos notáveis, aos conflitos internacionais, que fomentam novas tecnologias e buscam formas inovadoras para se fazer algo ordinário.

2.1 A História da Internet no Mundo

Segundo a definição do Dicionário Aurélio, internet é (2004, s.p):

> Qualquer conjunto de redes de computadores ligadas entre si por roteadores e gateways, como, p. ex., aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico (q. v.), o chat (q. v.) e a Web (q. v.), e que é constituída por um conjunto de redes de computadores interconectadas por roteadores que utilizam o protocolo de transmissão TCP/IP.

Conforme reportagem da jornalista Véronique Dumas, do site uol/historiaviva, a rede mundial de computadores (2012, s.p.):

> nasceu no final dos anos 1960, em plena Guerra Fria, graças à iniciativa do Departamento de Defesa americano, que queria dispor de um conjunto de comunicação militar entre seus diferentes centros. Uma rede que fosse capaz de resistir a uma destruição parcial, provocada, por exemplo, por um ataque nuclear.

Conforme Paschoal Mauro Braga Mello Filho define (2007, p. 121):

> Com a guerra fria no auge e a possibilidade sempre presente de um conflito nuclear em escala global, havia nos Estados Unidos a preocupação em montar um sistema logístico auxiliado por computadores que concentrasse toda a informação estratégica, mas que não fosse vulnerável a um único ataque nuclear.

Dumas, naquela reportagem, explica o curioso significado da palavra web (2012, s.p.):

> o pesquisador Paul Baran concebeu um conjunto que teria como base um sistema descentralizado. Esse cientista é considerado um dos principais pioneiros da internet. Ele pensou em uma rede tecida como uma teia de aranha (web, em inglês), na qual os dados se movessem buscando a melhor trajetória possível, podendo "esperar" caso as vias estivessem obstruídas. Essa nova tecnologia, sobre a qual também se debruçaram outros grupos de pesquisadores americanos, foi batizada de packet switching, "troca de pacotes".

Pode-se dizer que esse foi o embrião da internet. Ato contínuo, aproximadamente entre os anos 1970 a 1980, faculdades Estadunidenses passaram a adotá-la como uma forma interativa de comunicação entre docentes e discentes.

A internet começou a alcançar uma popularidade maior apenas em meados dos anos 1990, segundo Véronique Dumas (2012, s.p):

> Uma etapa decisiva foi superada em 1990 com a criação, por um pesquisador do Conselho Europeu para a Pesquisa Nuclear em Genebra (Cern), Tim Berners-Lee, do protocolo HTTP (Hyper Text Transfer Protocol) e da linguagem HTML (Hyper Text Markup Language), que permitem navegar de um site a outro, ou de uma página a outra. A World Wide Web (www) lançou seu voo, e a internet se abriu ao público, empresas particulares e privadas. Uma multidão de sites apareceu.
> Com uma infraestrutura de comunicação teoricamente desprovida de autoridade central, a internet, todavia, seria gerida de um contrato com o governo americano, que havia financiado sua criação, e diversos órgãos que assegurariam seu crescimento. Foi o caso da Internet Assigned Numbers Authority (IANA), responsável pela gestão dos nomes dos domínios, o DNS (Domain Name System). Graças a ele, os endereços IP, constituídos de uma série de códigos (o endereço numérico atribuído a cada computador conectado à rede) são traduzidos em letras que compõem nomes identificáveis e memorizáveis.

A rede mundial de computadores, tal qual como a conhecemos hoje, incorpora uma ideia-chave, qual seja, se baseia em uma rede de arquitetura aberta.

Nesse sentido, o site brgiga, nos informa que (2013, s.p):

> Nesta abordagem, a opção pela tecnologia de qualquer rede individual não é ditada por nenhuma arquitetura de rede particular e sim escolhida

> livremente pelo provedor, que a torna capaz de entrar em rede com outras redes pela "Arquitetura de Internetworking". Até aquele período, havia apenas um método para agregar redes: a tradicional troca de circuitos onde redes se interconectavam no nível do circuito, passando bits individuais em base síncrona por um circuito ponta a ponta entre duas localidades. Numa rede de arquitetura aberta, as redes individuais podem ser separadamente desenhadas e desenvolvidas e cada uma pode ter sua interface própria que pode ser oferecida a usuários e outros provedores. Cada rede pode ser desenhada de acordo com o ambiente e os requerimentos dos seus usuários. Não há restrições em relação aos tipos de redes que podem ser incluídas numa área geográfica, apesar de algumas considerações pragmáticas ditarem o que é razoável oferecer.

Notem que, apesar de estar engatinhando, o embrião da rede mundial de computadores já se encontrava em franco desenvolvimento. A aposta nesse sistema se consolida com a previsão de desenvolvimento futuro de novas tecnologias.

Segundo Dumas (2012, s.p):

> Em 1969, a rede ARPAnet já estava operacional. Ela foi o fruto de pesquisas realizadas pela Advanced Research Project Agency (ARPA), um órgão ligado ao Departamento de Defesa americano. A ARPA foi criada pelo presidente Eisenhower em 1957, depois do lançamento do primeiro satélite Sputnik pelos soviéticos, para realizar projetos que garantissem aos Estados Unidos a superioridade científica e técnica sobre seus rivais do leste. A ARPAnet a princípio conectaria as universidades de Stanford, Los Angeles, Santa Barbara e de Utah. Paralelamente, em 1971, o engenheiro americano Ray Tomlinson criou o correio eletrônico. No ano seguinte, Lawrence G. Roberts desenvolveu um aplicativo que permitia a utilização ordenada dos e-mails. As mensagens eletrônicas se tornaram o instrumento mais utilizado da rede. A ARPAnet seguiu sua expansão durante os anos 1970 – a parte de comunicação militar da rede foi isolada e passou a se chamar MILnet. Outras redes, conectando institutos de pesquisas, foram criadas nos Estados Unidos, Grã-Bretanha e França. Faltava estabelecer uma linguagem comum a todas. Isso foi feito com o protocolo TCP/IP, inventado por Robert Kahnet e Vint Cerf em 1974. A ARPAnet adotou essa padronização em 1976. E assim começou a aventura da web com seu primeiro milhar de computadores conectados. O afluxo de usuários engendrou um fenômeno de sobrecarga. Em 1986, uma nova rede foi lançada pela National Science Foundation. A ARPAnet se juntou a ela quatro anos mais tarde.

Com o surgimento cada vez mais veloz das empresas provedoras de internet, e, consequentemente, de conteúdo, a rede passou a ser utilizada por praticamente todos os segmentos sociais. Com isso, surgiu uma enorme facilidade com que os usuários poderiam fazer buscas e pesquisas pelo vasto sistema cibernético, os estudantes, de todos os níveis, passaram a buscar informações para

angariar dados que seriam utilizados em seus trabalhos escolares, os jovens e os adolescentes a utilizavam para sua diversão, e, finalmente os adultos a utilizavam para incalculáveis outras possibilidades.

A década de 1990 mostrou-se como uma era de grande expansão da rede mundial de computadores e, para facilitar a navegação, cuja qual não possuía uma interface amigável, foram desenvolvidos vários navegadores, os chamados "*browsers*", que são programas especialmente construídos e desenvolvidos para acesso às páginas da internet, e que seriam determinantes para a consolidação desta nova forma de comunicação global.

O acesso a e-mails abriu um leque infindável de possibilidades, tanto do ponto de vista pessoal, quanto do profissional, pois seus usuários passaram a se comunicar de uma forma mais livre por entre este "novo mundo" que surgia. Enviar currículos virtuais para uma gama ainda maior de empresas passou a ser rápido, fácil e eficaz.

O "*e-commerce"*, que pode ser definido como todo tipo de operação de compra e venda realizada pela rede mundial de computadores, foi outra ferramenta que surgiu com o advento da rede. Foi, e ainda é, uma das formas de empreendedorismo que mais progride no planeta, tanto pela facilidade, quanto pela comodidade com que seus clientes podem efetuar transações comerciais que, até um tempo atrás, eram feitas pessoalmente. Com isso, geram-se excelentes possibilidades de crescimento desse tipo de comércio, bem como a melhora dos lucros das empresas que investem nesse novo mercado.

A internet se arraigou tanto em nossos afazeres cotidianos, que não nos imaginamos mais sem esta fascinante tecnologia.

Informações do sítio Tecmundo dão conta que, para dar suporte a este mundo virtual (2012, s.p.):

> são utilizados milhares de quilômetros de fibra óptica – que respondem por cerca de 99% das conexões do nosso planeta. Estes cabos submarinos contam com uma capacidade total de troca de dados tão incrível que, se utilizada de uma vez só, já ultrapassaria os 7 "terabytes" por segundo.
>
> Com isso, é possível percebermos que somente 1% da internet é coberta pelos satélites, uma vez que eles apresentam uma conexão bem mais lenta. Dessa forma, eles acabam trabalhando somente como uma espécie de "plano B", uma garantia para o caso de algum acidente com os cabos

> acontecer.

Ficou claro que o surgimento da rede mundial de computadores se deu, inicialmente, por motivos bélicos, depois para fins acadêmicos e que, por fim, se tornou uma ferramenta indispensável para a chamada globalização, ligando Estados, culturas e pessoas de quase todo o mundo, com exceção de países como a Coréia do Norte, cuja ditadura familiar totalitarista e unipartidária, apesar de possuir acesso total à internet, restringe o acesso por parte de seus cidadãos.

Logicamente que com o surgimento da rede, nosso país não ficaria de fora e foi, em meados de 1995, com a ajuda da Rede Nacional de Ensino e Pesquisa, que o acesso mais amplo se consolidou por aqui.

2.2 A História da Internet no Brasil

Em seu site oficial, a Rede Nacional de Ensino e Pesquisa relata a história da internet no país (2009, s.p):

> A RNP foi criada em setembro 1989 pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infra-estrutura de rede Internet nacional de âmbito acadêmico. A Rede Nacional de Pesquisa, como era chamada em seu início, tinha também a função de disseminar o uso de redes no país.
>
> Em paralelo à implantação de sua estrutura, a RNP dedicou-se a tarefas diversas, tais como divulgar os serviços Internet à comunidade acadêmica através de seminários, montagem de repositórios temáticos e treinamentos, estimulando a formação de uma consciência acerca de sua importância estratégica para o país e tornando-se referência em aplicação de tecnologias Internet. Em maio de 1995, teve início a abertura da Internet comercial no país. Neste período, a RNP passou por uma redefinição de seu papel, estendendo seus serviços de acesso a todos os setores da sociedade. Com essa reorientação de foco, a RNP ofereceu um importante apoio à consolidação da Internet comercial no Brasil. Foi criado o Centro de Informações Internet/BR para dar suporte no surgimento de provedores e usuários da rede. Mais de 3.000 questões relativas à Internet foram respondidas em seu primeiro ano de funcionamento. Inúmeras empresas fabricantes de bens de informática, tais como Compaq, Equitel, IBM, Philips etc., passaram a oferecer apoio concreto à RNP, fornecendo equipamentos, software e, mesmo, financiando atividades diretas do projeto. Em outubro de 1999, dez anos depois de ser criado o projeto RNP, os ministérios da Ciência e Tecnologia e da Educação (MEC) assinaram um convênio, o

> Programa Interministerial de Implantação e Manutenção da Rede Nacional para Ensino e Pesquisa (PI-MEC/MCT), com o objetivo de levar a rede acadêmica a um novo patamar.
>
> Os dois ministérios investiriam R$ 215 milhões na implantação e manutenção do backbone RNP2, uma infra-estrutura de rede avançada, capaz de atender às novas necessidades de banda e de serviços para ensino e pesquisa. A Associação Rede Nacional de Ensino e Pesquisa (AsRNP), criada neste mesmo ano pelos funcionários da RNP, conduziria o programa, sob orientação de um Comitê Gestor (CG-RNP) formado por representantes do MEC e do MCT. O backbone RNP2 foi oficialmente inaugurado em maio de 2000.Em janeiro de 2002, a AsRNP foi qualificada pelo governo federal como uma Organização Social. Com isso, ganhou maior autonomia administrativa para executar suas tarefas e o poder público ganhou meios de controle mais eficazes para avaliar e cobrar o alcance dos objetivos traçados para a organização.

Desse momento em diante, a “febre” da internet passou a contaminar de maneira globalizada todas as pessoas que conseguiam acesso a esta encantadora e revolucionária ferramenta. Não havia mais volta.

Conforme dito alhures, no Brasil, o acesso mais substancial foi constatado a partir do ano de 1995, pois, antes, o acesso era mais restrito a docentes, discentes, bem como a funcionários de universidades e instituições de pesquisa. Tanto as instituições governamentais, quanto as privadas também conseguiram acesso à rede devido a colaborações acadêmicas e de atividades não relacionadas ao comercio.

A partir de 1995, surgiu a oportunidade para que usuários fora das instituições acadêmicas também tivessem acesso às facilidades da rede, e que a iniciativa privada pudesse vir a fornecer tais serviços, o que deu origem a ascendência extraordinária que a internet passou a ter desde então.

A rede mundial seguiu seu caminho rumo à popularização e, à medida que começou a ser assunto das mídias televisivas e escritas de massa, passou a despertar interesses na disputa pelo recém-criado mercado brasileiro.

Com a popularização massificada da internet, empresas dos mais diversos segmentos passaram a investir em sítios na rede mundial de computadores, inclusive instituições bancárias passaram a explorar com mais afinco o chamado atendimento “on-line”, cujo custo para implantação e desenvolvimento de sistemas de segurança não era e não é baixo.

A partir do momento em que empresas tradicionais e instituições

bancárias sólidas se voltaram a este novo segmento comercial, também surgiu o interesse de um conhecido ramo de pessoas: os infratores.

Onde há dinheiro, há pessoas interessadas na obtenção fácil e também ilícita de tal bem econômico, o que deu surgimento a um ramo então novo no Brasil, o dos crimes virtuais.

3 DOS CRIMES PRATICADOS NA INTERNET

Com o acesso à rede mundial de computadores cada vez mais facilmente disponibilizado, uma parcela cada vez maior de brasileiros pode usufruir de todas as benesses que a internet disponibiliza. Porém, o lado nefasto também coexiste, vitimando milhões de internautas a cada ano.

Segundo o Site Convergenciadigital (2013, s.p.):

> Devagar o Brasil vai propiciando acesso à Internet e, segundo o IBGE, 83 milhões de brasileiros podem ser considerados 'internautas' – ao menos no conceito estatístico de pelo menos um acesso nos três meses antes da pesquisa. Como indicador significa que 42,1% da população usa a rede.

Com mais pessoas acessando o mundo virtual, mais suscetíveis estão de serem vítimas de uma ação nesse campo, e, consequentemente, mais infratores estão de olho nesse "mercado" criminoso da internet.

Podemos definir crime das mais variadas formas. Fernando Capez o define como podendo ser conceituado sob os aspectos matéria e formal ou analítico (2011, p. 125):

> Aspecto material: é aquele que busca estabelecer a essência do conceito, isto é, o porquê de determinado fato ser considerado criminoso e outro não. Sob esse enfoque, crime pode ser definido como todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social.
>
> Aspecto formal: o conceito de crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo. Considerar a existência de um crime sem levar em conta sua essência ou lesividade material afronta o princípio constitucional da dignidade humana.
>
> Aspecto analítico: é aquele que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime. A finalidade deste enfoque é propiciar a correta e mais justa decisão sobre a infração penal e seu autor, fazendo com que o julgador ou intérprete desenvolva o seu raciocínio em etapas. Sob esse ângulo, crime é todo fato típico e ilícito. Dessa maneira, em primeiro lugar deve ser observada a tipicidade da conduta. Em caso positivo, e só neste caso, verifica-se se a mesma é ilícita ou não. Sendo o

> fato típico e ilícito, já surge a infração penal. A partir daí, é só verificar se o autor foi ou não culpado pela sua prática, isto é, se deve ou não sofrer um juízo de reprovação pelo crime que cometeu. Para a existência da infração penal, portanto, é preciso que o fato seja típico e ilícito.

Tal definição se encaixa perfeitamente à noção que temos do que é o crime, tanto em seu aspecto físico, quanto em seu aspecto psicológico. Ocorre que, com o advento da rede mundial de computadores, com a sua rápida gradação à categoria de indispensáveis à globalização mundial, e, consequentemente, com o surgimento dos ilícitos praticados nesse novo mundo virtual, houve a necessidade de se adequar os conceitos até então conhecidos, para novos conceitos que seriam adequados à esta nova realidade.

No tocante aos chamados crimes virtuais, eles possuem acepções meramente virtuais, porém seus efeitos são claramente notados no mundo real. Hodiernamente, não há como se apartar essas duas definições, pois, inegavelmente, os crimes virtuais têm gerado grande reflexo no cotidiano dessa sociedade “on-line”.

No início remoto de suas atividades, a internet era considerada como um mundo totalmente abstrato, intangível, porém, em uma velocidade astronômica, a rede mundial de computadores se tornou um lugar indispensável para que pessoas das mais variadas classes sociais e faixas etárias, pudessem realizar suas pesquisas, elaborar seus trabalhos, procurar empregos, se comunicar, dentre infinitas outras formas de utilização. Porém, onde há interesse, há infratores para se aproveitar das fraquezas e brechas do sistema, o que veio a alimentar os famigerados crimes virtuais ou digitais.

A conceituação de crimes digitais fornecida pelo autor Gustavo Testa Corrêa é “todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar” (2003, p. 69).

Note que, apesar de ser de 2003, esta conceituação é bem atual, pois engloba, além das informações que estão inseridas nas memórias dos computadores, também as que estão em trânsito nas redes virtuais, e conclui que tais dados deverão ser acessados ilicitamente para a prática de um crime.

Tais elementos tecnológicos faz surgir uma nova forma de crime, ou seja, como exemplo temos os caracteres que compõem as senhas pessoais (password), tão amplamente utilizadas atualmente em qualquer tipo ordinário de transação eletrônica, e que são, por muitas vezes, a única forma de segurança do usuário, não trazendo a devida importância que os mesmos possuem, podendo ser comparados, proporcionalmente, aos nossos documentos pessoais.

O elenco de crimes cibernéticos é bastante vasto e variado, conforme poderemos notar a seguir.

3.1 Estelionato

O *caput* do artigo 171 do Código Penal pátrio define o estelionato como:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa.

Seguindo a definição supra, podemos definir o estelionato caracterizado pelo emprego de meios fraudulentos, como o que induz alguém em erro, para obtenção de vantagem ilícita. Consiste, portanto, no fato de quem, se utilizando de meio enganoso, ardil, causa, dolosamente, injusto dano patrimonial a outrem. Desta forma, para melhor se adequar ao tipo aqui retratado, poderia ser definido no ramo da informática, como fraude na informática, onde este teria todo o elenco então exposto, porém, realizado no mundo virtual ou por meio do auxílio da informática.

3.2 Propagação de Material Ofensivo

A Lei nº 7.716 de 1989, conhecida como Lei do Crime Racial, em seu artigo 20 apregoa que:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
>
> Pena: reclusão de um a três anos e multa.
>
> § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.
>
> Pena: reclusão de dois a cinco anos e multa.
>
> **§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza. Pena: reclusão de dois a cinco anos e multa.**

Em meados dos anos de 1980, houveram casos em que foram propagadas determinadas informações que enalteciam o racismo e também a violência, com a ajuda de meios tecnológicos, em especial dos computadores.

Situações bastante conhecidas aconteceram nos Estados Unidos da América, como por exemplo: a “Ku Klux Klan”, grupo racista criado em 1865, no sul dos Estados Unidos, que vestiam roupas brancas e capuzes e perseguiam negros ex-escravos, libertos na Guerra de Secessão; há também a “Resistência Ariana Branca” (grupo que defende a supremacia branca), bem como os “Skinheads” aonde a subcultura skinhead era originalmente baseada em elementos de moda, música e estilo de vida, sendo subvertida e que passaram a intervir em questões de política e em questões raciais, dentre outras organizações de neonazismo. Tais grupos notaram que seria muito mais fácil e rápida a divulgação dos seus trabalhos se fossem realizados com os meios de comunicação eletrônicos, ao invés dos tradicionais.

Nos anos 1990, o “boom” da Internet, foi acompanhado de material ilegal e prejudicial.

Remy Gama diz em seu livro/site que (2000, p. 10):

> Hoje o centro das atenções é: a pornografia infantil e a pedofilia, na rede internacional de computadores, Internet. A internet é responsável por 95% da pedofilia nos Estados Unidos. É dificílimo identificar quem produz e divulga a pedofilia na Internet, pois as fotos ou vídeos, mesmo que não exibidas em home pages tradicionais, já que os provedores de acesso estão atentos ao assunto, são espalhados por e-mail ou em qualquer ambiente da Internet onde seja possível o envio ou a troca de arquivos. A Internet está se tornando rapidamente o fator mais significativo de abuso sexual de crianças e o principal meio de troca de pornografia infantil.

O acesso em massa à rede, tornou a propagação de referidos materiais muito mais acessível, bem como, mais difícil de localizar seus autores. A propagação pela rede de fotos, vídeos, imagens, dentre outros, fez com que os já covardes autores de tais fatos, se multiplicassem e se aventurassem ainda mais na covardia, com a proteção de uma tela de computador e de um modem.

3.3 Espionagem

A espionagem pode ser caracteriza pela alteração dos programas do computador que pode ser efetuada pela alteração de seus dispositivos de armazenamento, ou hard disk, por outros falsos, provocando a alteração de sua programação originária, promovendo o acesso ao banco de dados, registros e etc. O acesso intencional e injustificado de um usuário não autorizado pelo proprietário ou mesmo operador de um sistema de computador pode constituir um comportamento criminal.

Segundo Remy Gama (2000, p.34):

> Quando a informação é subtraída levando-se a parte corpórea (fita, disco rígido, etc), as providências penais tradicionais, como o furto e a apropriação, não criam problemas para o sistema penal. Porém, quando as informações são copiadas rapidamente pelos sistemas de telecomunicações, sem a presença do agente, subtraindo-as, surge a questão sobre a extensão da aplicação da legislação penal. O termo propriedade insinua exclusividade, posse, enquanto que a informação tende a ser concebida como um bem público. No direito pátrio, o furto não requer comentários neste trabalho, já a denominação furto de informações merece algumas observações. Sendo bem móvel pode-se, usufruir, gozar, modificar, etc, ou seja, é propriedade. Havendo a alteração em programas de computador, por meio da espionagem, para a transferência ou subtração

> de informações e dados do computador para uma pessoa não autorizada, conclui-se pela existência do furto de informação. Seguindo esta linha de raciocínio a apropriação pode existir, quando os dados ou informações não forem subtraídos, mas sim, copiadas por meio de artifícios eletrônicos mantendo-as intactas, sem que seu proprietário perceba que estas foram clonadas.

Atualmente, muito se especula até que ponto a espionagem virtual pode afetar a soberania de um Estado, como o ocorrido recente envolvendo os Estados Unidos da América e nosso país, episódio em que, este, tivera algumas bases de banco de dados “invadida” por aquele, o que gerou uma série de dissabores e contratempos diplomáticos.

3.4 Fraudes Virtuais

É vastamente utilizada em casos de ilícitos na área econômica, como o forjamento de saldos de contas, balancetes em bancos, transferências de dinheiro, etc, alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. As fraudes virtuais são os crimes de computador mais comuns, mais fácil de serem executados, porém, um dos mais penosos de serem esclarecidos. Não requer um conhecimento tão bem abalizado no que tange a informática e pode ser cometido por qualquer usuário que consiga acesso a um computador conectado à internet. Tradicionalmente, referida fraude, envolve a utilização de dados bancários furtados ou mesmo roubados.

De acordo com Remy Gama, existem leis específicas em alguns países sobre fraudes virtuais, como a Austrália, Áustria, Dinamarca, Alemanha, Finlândia, Luxemburgo, Japão, Holanda, Noruega, Espanha, Suécia e Estados Unidos. (2000, p. 8).

Segundo Luiz Gustavo Caratti de Oliveira, do site Ambitojurídico (s.d, s.p):

> em meados de maio de 2000, representantes do G-8, grupo que reúne os sete países mais industrializados do planeta e a Rússia, tentaram criar uma

> ciberpolícia, um órgão que teria a tarefa de combater as fraudes na internet, eis que os delitos no ciberespaço têm a particularidade de serem cometidos à distância, muitas vezes de um país para outro, mas a proposta foi rejeitada por questão de soberania de cada país e, receio de supremacia e de consagração de domínio dos EUA, que comandaria a polícia cibernética mundial.

O fato é que cada país deve adotar suas próprias medidas de combate aos crimes virtuais, pois, se diferente for, em pouquíssimo tempo, nosso Estado será duramente afetado por este câncer cibernético que se espalha na rede.

Ademais, de nada adianta sermos inexpugnáveis internamente, se os demais países forem negligentes tecnologicamente, pois o conceito de internet engloba também o da globalização.

4 DOS CRIMES VIRTUAIS MAIS PRATICADOS NO BRASIL

Os crimes que com mais frequência podem ser praticados na rede mundial de computadores são os crimes contra a honra. Vale lembrar que a Lei nº 5.250/67, a chamada Lei de Imprensa, fora declarada inconstitucional pelo Supremo Tribunal Federal (ADPF 130-7), sendo, portanto, os crimes contra a honra os elencados nos artigos 138 a 141 do Código Penal pátrio. Analisando tais dispositivos legais, pode-se chegar à conclusão de que determinadas manifestações e a propagação de opinião na internet podem vir a configurar os crimes de injúria, difamação ou mesmo calúnia.

4.1 Injúria

Conforme o texto legal utilizado pelo Código Penal, a injúria é caracterizada quando determinada opinião declarada por alguém, ofende o decoro ou a dignidade da pessoa. ”Art. 140 - Injuriar alguém, ofendendo lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa”.

Conforme nos ensina Fernando Capez (2012, p.184):

> A ação nuclear do tipo penal consubstancia-se no verbo “injuriar”, que é, conforme a definição de Nélson Hungria (1958a, v. 6, p. 90), “a manifestação, por qualquer meio, de um conceito ou pensamento que importe ultraje, menoscabo ou vilipêndio contra alguém”. Trata-se de crime de ação livre. Todos os meios hábeis à manifestação do pensamento podem servir à injúria: a palavra oral ou escrita, a pintura, o gesto etc.
>
> A injúria, ao contrário da calúnia e da difamação, não se consubstancia na imputação de fato concreto, determinado, mas, sim, a atribuição de qualidades negativas ou de defeitos. Consiste em opinião pessoal do agente sobre o sujeito passivo, desacompanhada de qualquer dado concreto.
>
> Por vezes, a injúria pode configurar desacato (art. 331 do CP) ou ultraje a culto (art. 208 do CP), isso porque tais crimes também consistem em violação à dignidade ou decoro pessoal; o crime de desacato, contudo, constitui um delito contra a Administração. No tocante ao crime de ultraje ao

> culto (“escarnecer de alguém publicamente, por motivo de crença ou função religiosa”), há um interesse social em proteger o sentimento religioso, de modo que a ofensa pública contra alguém por motivo de crença ou função religiosa configura o crime do art. 208 do CP, e não o crime de injúria.

Temos como exemplo, infelizmente bastante comum, a publicação e divulgação de textos e escritos de cunho racista nas chamadas redes sociais. Nesses casos, haverá aumento de pena, conforme o artigo 141, III, do Código Penal:

> **Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:**
>
> I - contra o Presidente da República, ou contra chefe de governo estrangeiro;
>
> II - contra funcionário público, em razão de suas funções;
>
> **III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.**
>
> IV - contra pessoa maior de 60 (sessenta) anos ou portadora de deficiência, exceto no caso de injúria. (Incluído pela Lei nº 10.741, de 2003)
>
> Parágrafo único - Se o crime é cometido mediante paga ou promessa de recompensa, aplica-se a pena em dobro.

Ora, não poderia ser diferente, pois a rede mundial de computadores, como poderosa ferramenta que é, facilita, e muito, a propagação de todo e qualquer material exposto na mesma, tendo o código penal acertado nesse sentido.

4.2 Difamação

Já o crime de difamação se configura com a imputação de fato ofensivo à reputação de outra pessoa. “Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa“.

Capez nos ensina que (2012, p. 179):

> O núcleo do tipo é o verbo “difamar”, que consiste em imputar a alguém fato ofensivo à reputação. Imputar consiste em atribuir o fato ao ofendido. A

> reputação diz respeito à opinião de terceiros no tocante aos atributos físicos, intelectuais ou morais de alguém. É o respeito que o indivíduo goza no meio social. A calúnia e a difamação ofendem a honra objetiva, pois atingem o valor social do indivíduo. Trata-se de crime de ação livre, que pode ser praticado mediante o emprego de mímica, palavra (escrita ou oral), ressalvando-se que, se realizada por intermédio de meios de informação (serviços de radiodifusão, jornais etc.), constituía crime previsto no art. 21 da Lei de Imprensa (vide comentários constantes do item 2.1., o qual trata da ADPF 130, tendo por objeto a referida Lei).
>
> Não importa que a imputação do fato seja falsa, ao contrário da calúnia, de modo que haverá crime ainda que o fato divulgado seja verdadeiro. O fato imputado não se deve revestir de caráter criminoso, do contrário restará configurado o crime de calúnia. A imputação de fato definido como contravenção penal caracteriza o crime em estudo. O fato deve ser concreto, determinado, não sendo necessário, contudo, descrevê-lo em minúcias. A imputação vaga e imprecisa, em termos genéricos, por outro lado, não configura difamação (nesse sentido: STJ, RT 714/418), podendo ser enquadrada como injúria. O fato ofensivo deve necessariamente chegar ao conhecimento de terceiros, pois o que a lei penal protege é a reputação do ofendido, o valor que o indivíduo goza na sociedade, ao contrário da injúria, em que há a proteção da honra subjetiva, bastando para a configuração do crime tão só o conhecimento da opinião desabonadora pelo ofendido.

Há que se dizer que, as supostas “ofensas” proferidas pelas partes ou mesmo pelos seus patronos em juízo, em petições ou mesmo oralmente, não caracterizam tais crimes de injúria ou difamação, bem como as críticas literárias, que tampouco são puníveis, tudo conforme se pode notar no artigo 142 do Código Penal:

> Exclusão do crime
>
> Art. 142 - Não constituem injúria ou difamação punível:
>
> I - a ofensa irrogada em juízo, na discussão da causa, pela parte ou por seu procurador;
>
> II - a opinião desfavorável da crítica literária, artística ou científica, salvo quando inequívoca a intenção de injuriar ou difamar;
>
> III - o conceito desfavorável emitido por funcionário público, em apreciação ou informação que preste no cumprimento de dever do ofício.
>
> Parágrafo único - Nos casos dos ns. I e III, responde pela injúria ou pela difamação quem lhe dá publicidade.

Um caso bastante conhecido é o de uma jornalista, de nome Rose Leonel, que teve em 2006, fotos e números de telefones divulgados na internet, em sites pornográficos afirmando que a mesma era prostituta, tornando a vida da vítima e a de seus filhos um inferno sem fim. Até que finalmente no ano de 2010 o empresário responsável pela infração fora condenado em 1º instância, e em 2011

referida condenação fora confirmada no Tribunal de Justiça do Estado do Paraná.

O caso supra mencionado é tratado pormenorizado no livro “Manual do Detetive Virtual”, de Wanderson Castilho, onde este conclui que (2012, p. 25/26):

> O seu parceiro pode divulgar as fotos, em um momento de raiva ou decepção. A sua máquina ou celular podem ser roubados ou perdidos. E se as fotos por acaso caírem nas mãos de pessoas erradas, o risco de se multiplicaram é muito grande.

O que existe entre quatro paredes realmente deve ficar entre quatro paredes, porém, se imagens ou vídeos forem divulgados sem a devida autorização, isso configurará infração elencada no código penal e levará o autor a responder por todos os danos suportados pela vítima.

4.3 Calúnia

A calúnia, no entanto, é a forma mais grave dos delitos contra a honra, uma vez que se imputa falsamente a alguém fato definido como crime, podendo ser cometida, inclusive, contra pessoa já morta. Segundo definição do Código Penal:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
>
> Pena - detenção, de seis meses a dois anos, e multa.
>
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
>
> § 2º - É punível a calúnia contra os mortos.

Finalmente, o autor Fernando Capez, nos dá a lição sobre calunia (2012, p. 173/174):

> Ação nuclear do tipo é o verbo “caluniar”, que significa imputar falsamente fato definido como crime. O agente atribui a alguém a responsabilidade pela prática de um crime que não ocorreu ou que não foi por ele cometido. Trata-

> se de crime de ação livre, que pode ser praticado mediante o emprego de mímica, palavras (escrita ou oral), ressalvando-se que, se realizada por intermédio dos meios de informação (serviço de radiodifusão, jornais etc.), constituía crime previsto na Lei de Imprensa (vide, no entanto, Arguição de Descumprimento de Preceito Fundamental, ADPF 130, tendo por objeto a Lei n. 5.250/67). Ressalte-se, finalmente, que o fato será enquadrado no Código Eleitoral se a calúnia for lançada em propaganda eleitoral. As espécies de calúnia (JESUS, 2000a, p. 466) são: a) inequívoca ou explícita: o agente afirma explicitamente a falsa imputação, por exemplo: "fulano de tal é o sujeito que a polícia está procurando pela prática de vários estupros"; b) equívoca ou implícita: a ofensa não é direta, depreendendo-se do conteúdo da assertiva, por exemplo: "não fui eu quem, por muitos anos, se agasalhou nos cofres públicos"; c) reflexa: imputar o crime a uma pessoa, acusando outra, por exemplo, dizer que "um Promotor deixou de denunciar um indiciado porque foi por ele subornado". O indiciado também foi ofendido.

A ação penal contra os crimes aqui definidos deve ser iniciada pelo próprio ofendido, mediante o oferecimento da chamada queixa crime, de iniciativa privada. As exceções à regra são a injúria qualificada, que envolve racismo ou atinge pessoas menos favorecidas, e também a hipótese em que o crime é praticado contra funcionário público. Em tais casos a denúncia deve ser oferecida pelo membro do Ministério Público, e a ação é de cunho penal pública. No caso de o ofendido ser o Presidente da República, a pena será aumentada em um terço, e a ação dependerá de requisição do Ministro da Justiça.

Entrando na seara processual, o processamento de tais crimes pode ocorrer perante os chamados JECrin's (Juizados Especiais Criminais), à exceção da injúria qualificada. Em função do rito especial, o ofendido poderá propor ao autor do delito a composição amigável dos danos então suportados, que se traduz em uma proposta de acordo para o pagamento de uma indenização. Acaso não aceita referida composição, o membro do *Parquet* poderá oferecer a suspensão condicional do processo, pelo período de 2 a 4 anos, ou mesmo a transação, na qual o ofendido deverá prestar uma pena alternativa.

Pode-se destacar alguns exemplos extraídos de julgamentos de tribunais pátrios referente tais crimes. Recentemente, o Superior Tribunal de Justiça considerou que informações publicadas a respeito de denúncias criminais são consideradas fatos de interesse publico (Ação Penal 628, julgada em 12/05/2011). Assim, entende-se que a publicação de notícias que tratam de ações judiciais não pode ser considerada calúnia, difamação ou injúria, desde que tal informação seja neutra, que não haja dolo de prejudicar o acusado, mas tão somente a intenção de

informar os cidadãos interessados.

> AÇAO PENAL ORIGINÁRIA. QUEIXA-CRIME POR CALÚNIA, INJÚRIA E DIFAMAÇAO. NOTÍCIA PUBLICADA NO SÍTIO ELETRÔNICO DA PGR ACERCA DE DENÚNCIA OFERECIDA PELO MPF. AUSÊNCIA DE DOLO ESPECÍFICO. NOTÓRIOANIMUS NARRANDI. INEXISTÊNCIA DE JUSTA CAUSA. QUEIXA REJEITADA.
>
> 1. A divulgação de notícia no sítio eletrônico da Procuradoria-Geral da República acerca do teor de denúncia oferecida por membro do Ministério Público Federal, com referência a circunstâncias levantadas pelo órgão acusador para perfazer a *opinio delicti* , com notório *animus narrandi* , não se mostra abusiva, tampouco viola a honra dos acusados.
>
> 2. A queixa-crime não traz consigo a demonstração do elemento volitivo ínsito à conduta criminosa, ou seja, não demonstra a inicial acusatória a existência de dolo específico necessário à configuração dos crimes contra a honra, razão pela qual resta ausente a justa causa para o prosseguimento da persecução criminal.
>
> 3. Queixa-crime rejeitada.
>
> ACÓRDAO: Vistos, relatados e discutidos estes autos, acordam os Ministros da CORTE ESPECIAL do Superior Tribunal de Justiça, na conformidade dos votos e das notas taquigráficas a seguir, prosseguindo no julgamento, após o voto-vista do Sr. Ministro Cesar Asfor Rocha rejeitando a queixa-crime, no que foi acompanhado pelos Srs. Ministros Felix Fischer, Gilson Dipp, Francisco Falcão e Nancy Andrighi, por maioria, rejeitar a queixa-crime, nos termos do voto da Sra. Ministra Relatora. Vencido o Sr. Ministro Massami Uyeda. Os Srs. Ministros Castro Meira, Humberto Martins, Maria Thereza de Assis Moura, Mauro Campbell Marques, Cesar Asfor Rocha, Felix Fischer, Gilson Dipp, Francisco Falcão e Nancy Andrighi votaram com a Sra. Ministra Relatora. Impedido o Sr. Ministro Arnaldo Esteves Lima. Ausentes, justificadamente, os Srs. Ministros Eliana Calmon, João Otávio de Noronha, Teori Albino Zavascki e Maria Thereza de Assis Moura.

No mesmo sentido, o julgado afirma que:

> Também não se vislumbra a ocorrência de crime de injúria, já que não houve a ofensa à honra subjetiva do querelante, com o desrespeito à sua dignidade da pessoa humana e ao seu decorro. Na verdade, a notícia não registrou atributos negativos ou defeituosos ao querelado, restringindo-se a comentários sobre a existência do "American Bar" e da aparente impossibilidade financeira de Lagos para justificar vultoso empreendimento com os vencimentos de funcionário público, o que, prima facie, justificaria a atuação do Ministério Público. Conforme acórdão extraído do Tribunal de Justiça de São Paulo (Recurso em Sentido Estrito n. 0015931-17.2008.8.26.0114). Do mesmo tribunal extrai-se que “comentários tecidos por desconhecidos no site da Prefeitura Municipal” não configuram crime contra honra, porque ausente o elemento subjetivo, o dolo (intenção inequívoca) de ofender ou difamar (Ação Penal Privada n. 0195240-78.2010.8.26.0000).

Acertado, ao meu ver, a decisão do tribunal bandeirante nesse julgado. Temos que levar em consideração que, todos temos o direito à informação e, no caso supra, a divulgação de determinadas notícias não configurou crime contra a honra, pois ausente está o elemento subjetivo, qual seja, o dolo.

4.4 Venda ou Exposição à Venda de Fotos, Vídeos ou Outro Registro, Envolvendo Criança ou Adolescente

A internet também pode propiciar a praticada de crimes de natureza muito mais graves, como a propagação e até mesmo a comercialização de vídeos e fotos pornográficas envolvendo menores, crime este previsto no art. 241 e seguintes do Estatuto da Criança e do Adolescente, Lei nº 8.069/90:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008). Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)

As penas previstas para este tipo de delito variam de 4 a 8 anos. Na verdade, se formos pela literalidade do dispositivo legal, o crime supra poderia ser imputado também aos provedores e servidores que dão acesso à internet (art. 241-A, parágrafo 1). Porém, este dispositivo dificilmente terá aplicação na prática, devido à falta de objetividade em se apontar o responsável pelo delito, dada a dificuldade em se individualizar o seu autor. E finalmente, pode-se incriminar também aquele que adquire ou mantém arquivado materiais pornográficos, conforme o art. 241-B do ECA, e pode ser condenado à pena de 1 a 4 anos.

> 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: (Incluído pela Lei nº 11.829, de 2008) Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)

Nunca é demais dizer que merece um maior rigor na prevenção e punição desse tipo de crime que envolve criança e adolescente, pois é o lado frágil de qualquer relação e merecem todo tipo de apoio, atenção e proteção, seja dos cidadãos, seja do governo.

4.5 Violação de Direito Autoral

Já, no que tange à violação dos direitos autorais, ou seja, a reprodução e distribuição de obras sem a devida autorização, está tipificada no artigo 184 e parágrafos do Código Penal. A matéria em tela é ainda controversa nos Tribunais frente ao princípio da adequação social, considerando-se o vasto comércio de vendas de CD`s e DVD`s piratas e à distribuição em massa de filmes, livros e vídeos através da rede de computadores. Aceito socialmente ou não, o fato é que reproduzir obras sem autorização do responsável pela mesma, ou não pagar por isso, é crime, punido com penas que variam de 3 meses a 4 anos de reclusão.

> Art. 184. Violar direitos de autor e os que lhe são conexos: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> § 1o Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> § 2o Na mesma pena do § 1o incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente. (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> § 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do

> autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 10.695, de 1º.7.2003)
>
> § 4o O disposto nos §§ 1o, 2o e 3o não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto. (Incluído pela Lei nº 10.695, de 1º.7.2003)

A violação de direitos autorais dos criadores de softwares, que são as ferramentas indispensáveis ao desenvolvimento da área tecnológica, copiando ou mesmo reproduzindo para fins comerciais, é definida como crime e está previsto no artigo 12 da Lei nº 9.609 de 1998, lei esta que trata da proteção à propriedade intelectual e da comercialização de programas de informática.

> Art. 12. Violar direitos de autor de programa de computador:
>
> Pena - Detenção de seis meses a dois anos ou multa.

A pena para este tipo penal, conforme se pode notar, é fixada em seis meses a dois anos ou multa, para a violação, e 1 a 4 anos e multa, em caso de reprodução para fins comerciais.

4.6 Outros Crimes Conexos

Além dos crimes supra mencionados, diversas outras condutas do Código Penal podem ser praticadas ou mesmo facilitadas mediante o uso da rede mundial de computadores. Dois exemplos bastante difundidos e, infelizmente, comuns, são a corrupção ou o aliciamento de menores bem como os crimes envolvendo a prostituição.

Não podendo se esquecer do estelionato, que pode ser realizado nas compras com o uso de cartão de crédito ou débito, e também com o uso de dados

alheios, bem como da extorsão por mensagens eletrônicas, também da formação de quadrilha e finalmente pelo furto das mais variadas formas. Todos esses tipos de crimes podem ser praticados e facilitados com o auxílio da internet.

Outro crime que se alastra muito rapidamente nos meios digitais é o chamado cyberbulling, que pode ser explicado como sendo a prática orquestrada através dos meios virtuais visando levar a vítima à humilhação bem como ridiculariza-los perante esta própria comunidade virtual, porém, com resultados que vão além da internet.

No nosso cotidiano, são inúmeras as informações que são inseridas na rede mundial de computadores, tais como: nomes, endereços, telefones, senhas, correio eletrônico, arquivos, fotos e uma infinidade de outros dados que possuem importância na vida privada. Algumas dessas informações são simplesmente liberadas pelos próprios usuários de forma espontânea em sites de relacionamento, que se tornaram uma verdadeira febre mundial.

Ocorre que, sabendo disso, muitos infratores pesquisam tais redes sociais a procura de informações que lhe possam auxiliar na prática de determinadas ações ilícitas, tais como, furtos, roubos, sequestros, dentre outras práticas delituosas.

Pesquisa realizada no site da RSA Anti-Fraud Command Center (AFCC), divisão de segurança da EMC2 Corporation, dão conta que, entre os anos de 2011 e 2012, o Brasil consta na lista entre os que mais tiveram empresas e marcas vitimadas por crimes digitais. Nosso país fica atrás apenas dos Estados Unidos e do Reino Unido, contabilizando 6% dos referidos crimes.

Essa pesquisa constatou apenas o que se já imaginava, ou seja, que tais crimes estão em ascendência, e que são facilitados, muitas vezes, pelo comportamento sem malícia e por vezes, exibicionista dos próprios usuários.

Tais crimes tão difundidos e conhecidos em nosso país teve, segundo o autor Sandro D'Amato Nogueira, como primeiro caso (2008, p. 29/30):

> na data de "28/08/1997 famosa jornalista da TV Cultura recebeu 105 mensagens (e-mails) de cunho erótico-sexual além de ameaçador a sua integridade física. As msg (sic) foram recebidas a partir das 00h31min24seg do dia 21 de agosto de 1997, quinta-feira, encerrando as 00h52min22seg do

> mesmo dia, numa média de uma mensagem a cada 11,9 segundos, o que, em princípio, indicava ter o ameaçador utilizado de programa específico de envio de mensagens simultâneas (MAIL BOMB).
>
> O referido acusado fora surpreendido, na manhã do dia 28 de agosto, em sua residência, quando se preparava para ir trabalhar. Não houve qualquer reação, entramos na residência e vistoriamos o seu computador, sendo possível localizar um programa de computador fantasma chamado Unabomber, e especialmente criado para o envio de milhares de mensagens simultâneas, além de mudar o nome do usuário dando, assim, uma aparência apócrifa ao criminoso virtual. Numa análise mais apurada do computador, foi possível encontrar o texto "texto.txt", onde estava a cópia da mensagem que foi enviada à vítima. Descobrimos também outra mensagem, com o mesmo conteúdo, mas endereçada a uma pessoa de prenome (...), sendo eu, diante das evidências, não restou ao acusado outra opção senão confessar a autoria do delito, dizendo, ainda, que além das ameaças encaminhadas aquela jornalista, enviou outras para uma famosa Jornalista da Folha de São Paulo. Meses depois o acusado, um excelente analista de sistema, foi condenado pelo Juiz do Forum da Lapa a prestar serviços junto a Academia de Polícia Civil, dando aulas de informática para novos policiais.

O trecho supra citado foi extraído da obra, intitulada "Crimes de Informática", cujo trecho transcrito faz parte integrante de uma entrevista em que o Delegado Mauro Macedo de Lima e Silva relata o primeiro caso de crime pela internet no país.

4.7 Da Violação ao Artigo 5º, X da Constituição Federal e ao Artigo 153, §1º A, do Código Penal

Pode-se afirmar que, uma vez inseridos os dados na rede, os mesmos nunca mais serão apagados. Isso se dá por conta de caches e cookies (sistemas de armazenamento de dados internos) que ficam armazenados nas memórias dos computadores que irradiaram a informação, bem como em todos os computadores que tiveram acesso à mesma informação então disponibilizada. Assim, qualquer hacker, cracker ou pessoa mais especializada, conseguirá acessar qualquer dado, a qualquer momento. Ocorre que, a violação a qualquer dado pessoal ou privado, viola nossa carta magna, em seu artigo 5º, inciso X:

> 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:
>
> (...)
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Bem como ao artigo 153, §1º A, do Código Penal:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
>
> Pena - detenção, de um a seis meses, ou multa.
>
> § 1º Somente se procede mediante representação. (Parágrafo único renumerado pela Lei nº 9.983, de 2000)
>
> § 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)
>
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

Um exemplo bastante ilustrativo se deu recentemente num caso em que uma mulher acabou por abandonar seu cachorro de estimação em uma movimentada avenida da cidade de São Paulo, e que, no momento em que a mesma dispensou referido animal para fora do veículo, fora flagrada por um casal que estava no veículo logo atrás, momento em que começaram a filmar toda a ação, e, ato contínuo, disponibilizaram as filmagens no site de compartilhamento de vídeos denominado Youtube, o que gerou uma comoção nacional e rendeu à autora da crueldade contra o animal, em princípio, um inquérito policial, bem como a ira de determinadas pessoas avessas a tal comportamento.

Ocorre que, um grupo de crackers denominados “anonymousbrasil” disponibilizou em seu site, facilmente listável em qualquer buscador, alguns dados privados da referida pessoa que abandonou o cão. Tais dados incluem: nome, número no cadastro de pessoas físicas (CPF), data de nascimento, telefones fixos e móveis, endereço residencial bem como os últimos locais em que a mesma trabalhou, gerando para esta, toda a sorte de dissabor que se possa imaginar.

Os crackers supra mencionados possivelmente se utilizaram de uma ferramenta denominada “Onion Browsers”, que são navegadores usados na

chamada Deep Web, ou seja, o submundo da internet, aonde tais usuários dificilmente são identificados, pois o protocolo da internet (Internet Protocol) não é rastreável facilmente, o que torna as ações realizadas por este grupo, quase que totalmente anônimas.

É claro que este exemplo é de um caso extremo em que o uso indevido dos dados pessoais foi utilizado, porém, todos os dias as pessoas disponibilizam seu dados em vários sites, sem se preocuparem em serem atingidas por este tipo de infrator virtual.

Está em tramitação na câmara, um projeto de lei de número 6541/2002, que Inclui como crime passível de pena a divulgação ou comercialização de endereços e dados pessoais sem a devida autorização.

Claro que existem casos em que os próprios envolvidos possuem a plena ciência de que estão em uma situação de total visibilidade, porém, não pensam duas vezes antes de se esporem, como é o caso, já mencionado, de pessoas que disponibilizam fotos pessoais a todo tempo nas redes sociais, chamando a atenção de infratores para casos de roubo, sequestro, extorsão, dentre outros.

Para se evitar tais dissabores, há a necessidade de se avaliar com acuidade se tais informações disponibilizadas na rede são realmente necessárias para se efetuar alguma transação, tendo como exemplo os cadastros obrigatórios realizados nas transações virtuais.

4.8 Considerações Finais

Mesmo com tais cuidados não estamos livres de ataques maliciosos. Existe, já a algum tempo, a venda ilegal de cadastros pessoais, nos quais constam uma gama de informações a respeito dos usuários, que, para efetuarem uma compra ou transação na internet, os fornecem, de forma obrigatória, à sites dito “seguros”, porém, mesmo com tal selo de segurança, referidas informações são “vazadas” e chegam ao alcance de empresas e pessoas mal intencionadas, que os

comercializam para um número incalculável de sites que realizam os chamados envio de “malas diretas”.

Pode-se definir “mala direta” como o envio, não solicitado, de alguma propaganda ou serviço ao consumidor, que, quase que diariamente, enchem nossas caixas postais eletrônicas com publicidade inútil e, geralmente, com conteúdo suspeito.

Há que se deixar claro que nosso país ainda está engatinhando no tocante à uma legislação que tenha como foco os chamados crimes virtuais, inclusive com leis recentes que especificam vários desses delitos.

Atualmente encontram-se em andamento, tanto no Executivo quanto no Legislativo, estudos e projetos de lei para regulamentar o uso consciente da rede mundial de computadores, tendo como maior exemplo o Marco Civil da Internet.

No tocante ao Poder Executivo, estuda-se a instituição do referido Marco Civil da Internet, projeto esse que define direitos e responsabilidades de provedores, usuários, bem como do Estado no acesso à rede. Tal projeto de lei, de nº 2.126 de 2.011, fora enviado à Câmara dos Deputados em no dia 24 de agosto de 2011 e até hoje ainda não foi aprovado.

Na mesma Câmara, encontra-se o Projeto de Lei nº 84 de 1.999, que dispõe sobre os crimes cometidos na área de informática e suas penalidades. Neste projeto foram inseridos diversos crimes relacionados exclusivamente com o uso da internet, como a lesão ou obtenção indevida de dados, alteração de senhas (passwords), o acesso não autorizado, falsificação de dados e também a divulgação de imagens privadas. Há mais de 15 anos o projeto encontra-se em tramitação, não havendo previsão para a sua aprovação.

Porém, tem que se ter em vista que, apesar destas leis específicas estarem indo ao encontro dos avanços tecnológicos, tais avanços estão evoluindo a cada semana, o que tornam tais normas legais um tanto quanto defasadas rapidamente, gerando uma obsolescência legal.

Outro ponto nevrálgico a ser explorado, é o fato de que, não nos adianta se tais leis seguirem a velocidade alucinante dos crimes cibernéticos, se os próprios usuários não se policiarem diuturnamente, como por exemplo, não expondo seus dados a sites não confiáveis, bem como, não expondo, deliberadamente,

informações em redes sociais.

Em matéria veiculada na Revista do Advogado número 115, na matéria assinada por Fabiana Regina Siviero e André Zanatta Fernandes de Castro, os mesmos colocam que (2012, p. 55/56):

> Pessoas públicas, celebridades e políticos se expõem voluntariamente em troca de promoção. Aguçam o interesse das pessoas a seu respeito mediante renúncia à parcela da intimidade cuja proteção lhes é constitucionalmente assegurada. Vivemos também a era das "celebridades" instantâneas, famosas de um dia para o outro na internet, tais quais bebês risonhos expostos por seus pais em vídeos com milhões de exibição. É inegável que ao tutelar o direito à privacidade, os arts. 5º, inciso X, da Constituição Federal (CF), e 12 e 21 do Código Civil (CC) não criam uma redoma de proteção absoluta ao redor das pessoas. De outro lado, o direito individual à privacidade será sempre sopesado em relação aos direitos amplos à informação, à cultura e à liberdade de expressão, igualmente princípios constitucionais (CF, arts. 5º, inciso XIV, 215 e 220).

Some-se a essas informações o fato de que uma grande parcela das pessoas que utilizam as chamadas redes sociais são "analfabetos funcionais", surgindo um grande problema a ser enfrentado pelas leis pátrias, ou seja, o crescimento desordenado de crimes dessa natureza.

5 DA ANÁLISE DA LEI N° 12.737 de 2012

A recente Lei nº 12.737 de 2012, que preceitua acerca da tipificação criminal de delitos informáticos é um excelente exemplo de que estamos indo ao encontro da evolução legal nessa seara. Carolina Borges Rocha reflete bem o que se entende das novas condutas criminosas expostas na referida lei (2013, p. 1):

> O debate sobre os crimes na internet se mostra relevante, haja vista que com a evolução tecnológica, a informática, em especial a internet, se tornou um meio hábil e eficaz de comunicação e informação, transformando, assim, o cotidiano do homem moderno. Sucede que esta modernização estendeu-se também sobre o Direito, em especial no campo do Direito Penal.
>
> No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal de 1940 tende a lidar com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra à honra, dentre outros.

A Lei nº 12.737 de 2012, que acrescenta dois artigos ao Código Penal (154-A e 154-B), e altera outros dois outros artigos (266 e 298) se tornou um ícone da proteção à intimidade por ter sido aprovada ante uma invasão de intimidade virtual de uma celebridade televisiva, o que fez com que tal dispositivo legal se tornasse tão difundido e conhecido em tão pouco tempo.

Popularmente chamada de Lei Carolina Dieckmann, por ter sido esta atriz que gerou o estopim da aprovação, referida lei se baseia num antigo projeto chamado Lei Azeredo.

Mariana Congo, do blog Estadão, informa que (2013, s.p.):

> O texto original da Lei Azeredo envolvia questões polêmicas, como a obrigação dos provedores de fiscalizar e guardar os registros da atividade de usuários, ou o fato de tornar crime o compartilhamento de arquivos.
>
> A Lei Carolina Dieckmann surgiu como alternativa à Lei Azeredo e foi aprovada em poucos meses.

Tal dispositivo legal, sancionada pela Presidente Dilma Rousseff, dispõe sobre a tipificação criminal de delitos informáticos, qualificando como crimes determinadas ações através de meios eletrônicos ou virtuais, e que outrora, necessitavam ser adequados ou adaptados aos dispositivos legais então em vigor, o que, na maioria das vezes, não tinham adequação similar.

Agora, com mais facilidade, as autoridades públicas poderão tipificar os fatos delituosos aos seus correspondentes penais, aplicando-se assim a lei ao delito em concreto, tornando tais práticas delituosas menos atrativas aos seus infratores.

Em um dos artigos, o 154-A, cujo título é “Invasão de dispositivo informático”, a redação é a seguinte:

> 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.

Conforme se pode evidenciar, tal artigo trata de pontos bem específicos, tais como, violação de mecanismo de segurança, bem como os responsáveis por softwares maliciosos, aumentando-se a pena em caso de prejuízo econômico. Engloba também a falsificação de documentos, tal qual se verifica com os cartões de crédito, ou mesmo débito.

Ocorre que nem todos aplaudem por completo tal iniciativa. O Jurista Luiz Flávio Gomes, em seu artigo intitulado "A (in)eficácia da Lei Carolina Dieckmann" expõe que (2013, s.p):

> Consoante Bauman (texto citado), "o advento da sociedade-confessionário marcou o triunfo definitivo daquela invenção esquisitamente moderna que é a privacidade – mas também marcou o início das suas vertiginosas quedas do apogeu da sua glória. Triunfo que se revelou ser uma vitória de Pirro, naturalmente, visto que a privacidade invadiu, conquistou e colonizou a esfera pública, mas ao preço de perder o seu direito ao segredo, seu traço distintivo e privilégio mais caro e mais ciumentamente defendido.

Assim como a supra citada lei se tornou um marco na defesa dos ilícitos cometidos no espaço virtual, outro dispositivo legal fora criado para que seja estruturado pela policia judiciária, setores e equipes especializadas no combate à esse tipo de ações delituosas. Esta lei possui a seguinte redação:

> Art. 1o Esta Lei altera o Decreto-Lei no 2.848, de 7 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 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
>
> Art. 2o (VETADO)
>
> Art. 3o (VETADO)
>
> Art. 4o Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> Art. 5o O inciso II do § 3o do art. 20 da Lei no 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:
>
> "Art. 20. § 3º (...)
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
>
> Sem dúvida, tais dispositivos legais se mostrarão um avanço no sistema jurídico e legislativo pátrio o que colabora para a investigação, culminando

> no sentenciamento de referidos infratores cibernéticos.

Alguns países, já a algum tempo, buscam meios de viabilizar métodos mais eficazes de repressão e prevenção dos chamados delitos cibernéticos, que cada vez mais se alastram e se sofisticam, razão pela qual é necessário que se estabeleça uma legislação rígida, objetiva e adequada, a fim de que não se macule o princípio da legalidade ou mesmo se tornem impunes condutas relevantes do ponto de vista penal. Por exemplo, na Argentina, não existe legislação sobre o tema. Já na Espanha, ao contrário, existem várias normas legais que tipificam condutas relacionadas com a o mundo cibernético e seus crimes. Já no Chile, a Lei nº 19.223 de 1993 tipifica uma série de delitos relacionados com a informática, tendo como exemplos a sabotagem, a espionagem, etc. Nas Filipinas, de onde, possivelmente teria se originado o vírus ILOVEYOU (vírus de computador que afetou milhões de computadores Windows em 5 de maio de 2000. Seu nome oficial é LOVE-LETTER-FOR-YOU.txt. Se disseminou via e-mail), que causou bilhões de reais em prejuízos, os deputados tentam aprovar às pressas uma lei, com penas de seis meses a três anos de prisão para os infratores virtuais, além do pagamento de uma multa que seria proporcional aos danos então causados.

Wanderson Castilho apregoa que (2012, p. 68):

> Em alguns países, como Itália, o acesso indevido a redes de computador é punido pelo delito de “invasão de domicílio”, No Brasil, isso é impossível, considerando que em direito penal não se pode fazer analogia para prejudicar o réu.

Fica evidente que o combate a tais crimes cibernéticos demanda um investimento maciço em tecnologia da informação, tanto das provedoras, quanto do governo. Além disso, há de se criar nos usuários finais desses serviços, uma mentalidade mais ativa, do ponto de vista de não deixarem se levar por tudo o que ocorre na rede, criando, com isso, um juízo de valores mais racional e menos impulsivo na hora de se realizar transações ou mesmo nos relacionamentos virtuais.

6 DAS FORMAS DE SE PRESERVAR A SEGURANÇA E A INTIMIDADE NA REDE MUNDIAL DE COMPUTADORES

Não se pode dissociar as formas de segurança do chamado mundo virtual e do mundo real, pois existem similaridades em ambas.

Com o advento da internet banda larga e o uso massificado de tais tecnologias, inexoravelmente o mundo se voltou, e o Brasil não poderia ficar de fora, para esta maravilha moderna revolucionária. Tais usuários, então amadores, passaram a ser extremamente atualizados e antenados nos avanços tecnológicos e também nos métodos de segurança.

Outrora, e-mails falsamente enviados por supostas instituições sérias eram abertos com toda confiança, hoje, poucos são os casos desse tipo, apesar dos infratores serem bem criativos e tentarem criar artimanhas das mais engenhosas para atingir seus objetivos ilícitos.

Como já dito outrora, nesta nossa sociedade digital, a coleta de informações e dados se tornou uma prática bastante usual e necessária em qualquer segmento que se possa imaginar, tornando tais dados vulneráveis a ataques. Isso sem falar na comercialização em massa de máquinas fotográficas digitais e celulares com câmera fotográfica, que, tornou o hábito de se tirar fotos uma ação natural, inclusive em momentos de privacidade. Tais momentos podem ser divulgados para todo o mundo assim que tais dispositivos forem perdidos, furtados ou roubados e caírem em mãos de estranhos maliciosos e maldosos.

Uma pessoa mediana, no seu cotidiano, certamente não entregaria as chaves de sua residência para que um estranho adentrasse em seu lar e começasse a bisbilhotar suas gavetas, seus pertences, e etc. Ora, diferente não poderá ser quando falamos no mundo virtual, ou seja, ninguém deveria disponibilizar para pessoas estranhas e sem nenhuma confiabilidade, suas senhas e dados pessoais para que estas acessem sua máquina e faça uma devassa em seus arquivos.

Senhas e outros tipos de dados, certamente não podem ser disponibilizados em qualquer tipo de página virtual, ou seja, há websites que

podemos confiar, por todos os itens de segurança que os mesmos apresentam, e websites que não devemos confiar, como em qualquer transação física que realizamos.

No momento em que uma pessoa entra em uma agência bancária física, está claro que neste local existe toda uma esfera de confiabilidade e segurança para que se possa realizar suas transações bancárias em um ambiente livre de pessoas e de equipamentos maliciosos. Pelo menos é o que se espera. Diferente não poderia ser quando se acessa um sitio oficial de uma instituição bancária, cuja existência de dispositivos de segurança e softwares livres de ameaças tornam as transações mais seguras e confiáveis e fica claro que, a partir do momento em que referido cliente for vítima de ataques cibernéticos dentro de tal site, o mesmo terá direito ao ressarcimento integral do prejuízo sofrido.

No quesito segurança, a maioria das instituições bancárias possuem em seus sítios oficiais algumas medidas de segurança padrão, similares a que passo a expor.

6.1 Da Segurança nos Sites

Não são raros, infelizmente, as invasões em contas cadastradas no chamado Net Banking, ou seja, nos bancos virtuais, aonde seus usuários a acessam pelo computador. Nos sites em que se pode realizar transações financeiras, bem como nos sites de compras, os usuários devem ficar atentos a alguns elementos sem os quais sua atividade virtual poderá ser comprometida e até mesmo invadida. O Banco do Brasil, por exemplo, em seu site oficial, nos dá informações importantes a respeito de segurança (2013, s.p.):

> **NUNCA** informe o número do seu cartão ou o seu código de segurança ao utilizar o Auto-atendimento BB pela Internet. O Banco do Brasil jamais solicita essas informações pela Internet.
>
> **CERTIFIQUE-SE** de que está na área segura do portal BB, verifique a existência de um pequeno cadeado fechado na tela do programa de

navegação. Note também que no início do campo "endereço" surgem as letras "https".

EVITE atalhos para acessar o site do BB, especialmente os obtidos em sites de pesquisa. Digite sempre no campo do endereço.

PROCURE sempre acessar o site bb.com.br no início da conexão ao provedor. Evite navegar em outras páginas ou acessar "e-mail" antes de utilizar o auto-atendimento BB pela Internet.

EVITE realizar operações em equipamentos de uso público, eles podem estar com programas antivírus desatualizados ou preparados para capturar os seus dados.

EVITE abrir e-mail de origem desconhecida.

EVITE também executar programas ou abrir arquivos anexados, sem verificá-los com antivírus atualizado, mesmo que o conteúdo seja criado pela pessoa de sua confiança que os enviou. Eles podem conter vírus ou cavalos-de-tróia, sem que os remetentes sequer saibam disso.

SOLICITE aos seus amigos que não enviem mensagens de e-mail de corrente (spam). Essas mensagens normalmente oferecem facilidades promocionais, propaganda enganosa, curiosidades, mensagens de amizade e outros títulos, sempre orientando o reenvio para 10 ou mais amigos, e são muito utilizadas para propagar vírus e cavalos de tróia.

UTILIZE somente provedores com boa reputação no mercado e browsers e antivírus mais atualizados. A escolha de um provedor deve levar em conta também as políticas de segurança e a confiabilidade da empresa. **CERTIFIQUE-SE** de que realmente encontra-se na área segura do site do BB ao digitar sua senha BB Internet para realizar compras em sites que oferecem facilidades de débito em conta.

CERTIFIQUE-SE também de que as demais pessoas que utilizam o seu computador tenham conhecimento e sigam as orientações de segurança.

INFORME-SE sempre sobre as melhores práticas de segurança. Os endereços www.antispam.br e www.cartilha.cert.br pertencem a instituições conceituadas e trazem boas informações sobre o assunto.

CONSULTE sempre esta página para novas informações sobre a segurança dos canais de Auto-Atendimento do BB.

CONFIRA quando foi o seu último acesso.

SAIBA que o Banco do Brasil não envia mensagens de correio eletrônico a seus clientes, nem autoriza qualquer parceiro comercial a fazê-lo em seu nome. O BB respeita acima de tudo sua segurança e privacidade. Qualquer dúvida entre em contato com o SAC BB.

Podemos notar que tais informações contidas no site de referida instituição bancária, nos dão conta de que são precauções básicas e eficientes que tornam a navegação e também as transações virtuais bem mais seguras e capazes de serem realizadas sem maiores complicações e se evitando toda sorte de dissabores e aborrecimentos.

6.2 Das Formas de se Evitar Invasão

Usualmente, podemos nos deparar com algumas políticas de uso aceitável, ou seja, são políticas que se baseiam no uso racional e sensato dos usuários que contratam tais serviços, como por exemplo, ao contratar os serviços de uma provedora de internet, o usuário passa a aceitar determinados termos de uso para que não seja exposto à vírus e spams.

Podem-se elencar algumas situações e atividades que os usuários não devem realizar:

-divulgação de informações pessoais;

-compartilhamento ou mesmo envio de mensagens contendo spam e códigos maliciosos;

-compartilhamento de password (senhas);

-distribuição e cópia não autorizada de material protegido por direitos autorais;

-invasão a outros computadores;

A não observância a determinadas regras de referida política de segurança a que o usuário está sujeito, poderá ser considerado como uma falha de segurança, estando sujeito, por vezes, à rescisão contratual dos serviços prestados.

Numa analogia, podemos considerar tais desrespeitos ao sistema de segurança ou política de privacidade como uma verdadeira bola de neve, pois, se um usuário inobservar as politicas de segurança, a sua própria máquina será infectada, bem como, dependendo do vírus malicioso, poderá infectar todo servidor em que a máquina está hospedada, e com isso, infectando todos os computadores que estiverem hospedados no mesmo provedor.

Isso ocorre pois, quando uma máquina é infectada por um vírus, ela passa a ser um hospedeiro que será utilizado para enviar os famigerados “spams” que são mensagens não solicitadas e sem propósito. Com isso, torna o provedor de acesso mais lento, gerando congestionamento em boa parte de seu sistema.

6.3 Da Criptografia e das Ferramentas Antimalware

Outra ferramenta bastante divulgada e utilizada para se evitar ataques é a chamada criptografia, que é definida, em suma, pelo Professor Emerson Santiago como: “(do grego kryptos, oculto, e graphein, escrever) é o nome dado a um conjunto de regras que visa codificar a informação de maneira que só o emissor e o receptor consiga decifrá-la” (2012, s.p.).

E como este singelo trabalho de conclusão de curso não pretende esgotar o assunto em tela, pois não é esse o objetivo principal, por derradeiro, há que se citar as tais Ferramentas Antimalware, que é descrita pela empresa Microsoft como sendo (2012, s.p):

> Malware é um nome abreviado para “software malicioso” Malware é qualquer tipo de software indesejado, instalado sem o seu devido consentimento. Vírus, worms e cavalos de troia são exemplos de software mal-intencionado que com frequência são agrupados e chamados, coletivamente, de malware.
>
> Como proteger seu computador contra malware:
>
> Existem diversas maneiras de ajudar a proteger o seu computador contra malware: Garanta que atualização automática esteja habilitada para obter todas as atualizações mais recentes de segurança.
>
> Mantenha seu firewall ativado.
>
> Não abra mensagens de e-mail de spam, nem clique em sites suspeitos.

No que tange à intimidade no mundo virtual, não é errado afirmar que as ações dos próprios usuários são, na maioria das vezes, determinantes na invasão ao disponibilizarem dados e imagens em redes sociais, sobrando uma parte residual para as ações realmente ilícitas.

A intimidade de uma pessoa diz respeito apenas a ela e a quem ela concorde em compartilhar, porém, muitas vezes, tais pessoas se deixam ser registradas em fotos comprometedoras que acabam “vazando” para sites especializados. Isso, sem dúvida, acarreta uma invasão na privacidade alheia e deve ser devidamente punido.

6.4 Outras Soluções de Segurança

Uma solução para dar suporte a crimes ocorridos no mundo virtual e que pode servir para futuras ações judiciais, é, no momento em que se verificar a ocorrência desses ilícitos, se dirigir a um cartório, e realizar uma ata notarial do ocorrido. A vítima terá assim, uma prova robusta para uma futura ação judicial cabível.

Há que se deixar claro que, os dados inseridos em um computador, ou mesmo os protegidos por senhas nas famosas nuvens (cloud), não raramente, valem mais do que os próprios equipamento em que estão registrados, sendo as máquinas que os hospedam apenas embalagens de luxo que tem, por dentro, uma joia de valor inestimável.

Por isso quando o assunto é proteção à intimidade, essencialmente os usuários necessitam ficar atentos a quaisquer atitudes suspeitas no mundo virtual, como se fosse a atenção diária do mundo real, pois ameaças existem das mais variadas formas, porém, os mais sagazes e espertos se safam com mais facilidade.

Outro ponto importante diz respeito à forma como referido usuário se comporta em frente ao computador, ou seja, pessoas há que exacerbam em suas exposições nas redes sociais, geralmente pessoas carentes que encontram no conforto da internet, uma fortaleza não tão segura, o que passa a chamar ainda mais a atenção de pessoas maliciosas e com segundas intenções, podendo, por vezes, tais usuários serem “levados pela lábia”.

Por isso, o chamado Marco Civil da Internet, que está prestes a ser votado pelo Congresso Nacional, estabelecerá os direitos e os deveres dos usuários, o que certamente irá coibir a ampliação deste tipo de ações criminosas nesse campo.

Certamente que crimes de divulgação e propagação de imagens e dados pessoais, como o que ocorreu com a atriz Carolina Dieckmann, serão mais facilmente punidos, inclusive com a retirada imediata de tais imagens, independentemente de autorização judicial. Com isso, se evitará a propagação em

massa de tais dados, bem como casos em que as vítimas de referidos crimes, em função da exacerbada exposição, acabam sendo muito prejudicadas, chegando, inclusive, ao inimaginável, ou seja, dando cabo à própria vida.

7 ESBOÇOS DO MARCO CIVIL DA INTERNET

A violação à intimidade pode gerar mais que apenas vergonha para os envolvidos, podendo chegar até a morte, como o ocorrido com duas meninas, uma com 16 anos, de Veranópolis-RS, e uma com 17 anos, do Estado do Piauí, cujo fim trágico, se deu pela divulgação, não consentida, em rede social, de fotos e vídeos em que as mesmas apareciam de forma erótica, chegando ao ponto de darem cabo às próprias vidas.

Há que se salientar, porém, que, como nos casos citados, a responsabilidade pelo ocorrido certamente não foi imputada às envolvidas, porém, se não fossem suas atitudes negligentes e mesmo ingênuas, ante sua própria privacidade, tais fatos certamente não teriam ocorrido.

Conforme o próprio nome diz, o Marco Civil da Internet, assim que aprovado, certamente será a pedra fundamental em que os direitos e deveres relacionados ao mundo virtual terá respaldo e, a partir do momento em que for devidamente aprovado, quem se sentir ofendido ou turbado no seu direito à intimidade e privacidade, poderá requerer do responsável pela página da internet ou mesmo à provedora envolvida, que suspenda todo e qualquer acesso ao referido material objeto da discórdia.

Tal projeto, dentre seus artigos, prevê a exigência da guarda de todos os registros e documentos igualmente importantes de acesso de todas as empresas que atuem visando finalidade econômica na rede. O jornalista Tadeu Breda alerta que (2013, s.p.):

> Software livre, criptografia, garantias legais e contraespionagem: eis a receita de especialistas para diminuir a vulnerabilidade de empresas, cidadãos e instituições brasileiras ao monitoramento internacional de dados. “Apenas soluções técnicas não serão suficientes para resolver o problema da segurança”, adverte o ciberativista gaúcho Marcelo Branco, um dos fundadores da Campus Party no país. “Devemos usar programas de código aberto, ter órgãos de inteligência capazes de prever e evitar interceptações, além de uma legislação que jogue o vigilantismo na ilegalidade.

O texto acima retrata a preocupação para com os ataques cibernéticos no país. Tais preocupações e ações não devem ser apenas das empresas envolvidas, há que se mudar a cultura e as atitudes dos usuários da rede.

Pode-se destacar 3 pontos nevrálgicos do referido projeto de lei.

1- Da Privacidade: O Marco Civil da Internet assegura uma regra muito importante no que toca a privacidade dos seus usuários: as empresas de telecomunicações deverão se abster em guardar os dados de navegação de seus usuários, ou seja, por quais sítios e páginas referido usuário navegou. Claramente isso evitará que pessoas mal intencionadas vendam tais dados de rastreamento para terceiros, evitando o que se chama de “venda de dados”.

O artigo 3º do projeto de lei garante a disciplina do uso da rede mundial de computadores no Brasil a partir da proteção da privacidade e proteção aos dados pessoais, na forma da lei.

2- Da Neutralidade: Conforme o Site Marcocivil.org, pode-se definir a neutralidade como (s.d., s.p.):

> NEUTRALIDADE DA REDE é o princípio de que quem fornece os cabos e fibras de conexão não pode comercializar, bloquear, privilegiar ou interferir na escolha de conteúdos ou aplicativos do internauta.
>
> Um princípio defendido no texto original do Marco Civil.

E segue que, as operadoras de telecomunicação querem a autorização legal para monitorar, filtrar e bloquear as aplicações e mensagens que trocamos “on-line”, a fim de prever nosso comportamento na rede para criarem dificuldades e venderem facilidades na nossa navegação. Porém, a neutralidade da rede, garantida no Marco Civil, impede esse tipo de prática das operadoras, proibindo interferências indevidas no fluxo de dados e proibindo a discriminação ou privilégio de informações por razões comerciais ou quaisquer outras que não sejam meramente técnicas. A neutralidade garante conexão em alta velocidade (banda larga) sem diferenças nas contratações, seja pelos provedores de serviços da internet, seja pelos provedores de banda larga.

A referida neutralidade de rede sugere que o usuário tem o direito de acessar a informação que quiser, e diz respeito à liberdade com que as pessoas possuem de se comunicarem. Diz respeito também, e não poderia ser diferente, à liberdade de expressão no nosso tempo, pois protege o direito das pessoas criarem

websites, páginas, blogs, o que for, e poder alcançar outros usuários. É algo que consideramos implícito na internet, porém, sem isso, a rede não seria ativa como ela hoje o é.

3- Da Liberdade de Expressão: É de suma importância que a lei garanta a liberdade de expressão, certamente, sem ferir o direito de outras pessoas.

Segundo o site supra, o projeto de lei do Marco Civil prevê diversos artigos que corroboram a necessidade da emissão de "ordem judicial" o que dá legitimidade aos atos jurídicos necessários. Temos como exemplos os artigos 7º, 10 e 15 (s.d, d.p.):

> O artigo 7º estabelece que "o acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados" os direitos: "à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal";
>
> O artigo 10, em seu parágrafo 1º, garante que o provedor responsável pela guarda "somente será obrigado a disponibilizar as informações que permitam a identificação do usuário mediante ordem judicial se: houver fundamento dos indícios da ocorrência do ato ilícito; para fins de investigação ou um processo judicial; houver determinação de um período específico que ocorreram os registros.
>
> O artigo 15 assegura a liberdade de expressão e evita a censura, uma vez que o provedor de aplicações de Internet (aplicação de software ou sistemas de informática) "somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências."

Nosso país, certamente está indo ao encontro de novos dispositivos, tanto legais quanto tecnológicos para se adequar aos novos desafios por que passa o planeta.

Avanços na área de informática nunca foram um problema para os desenvolvedores pátrios, porém, o problema se dá no momento de se aplicar determinada tecnologia a uma instituição pública ou mesmo no momento de se alterar determinadas rotinas que duraram décadas, para se tornarem eficientes.

No que toca aos avanços legislativos, naturalmente mais lentos, vide o nosso arcaico Código Penal de 1940, o que vemos atualmente é um importante avanço nessa matéria, pois, leis e projetos de leis estão borbulhando nas casas legislativas, e, não sem tempo, pois lá se vão, aproximadamente, 20 anos desde que a internet aportou de vez em nosso solo, sem que tivéssemos nenhuma lei

específica e objetiva para tratar de tais assuntos tão delicados e de difícil solução.

A aprovação de um Marco Civil da Internet que avance na garantia dos direitos dos usuários à privacidade também é apontada como uma das medidas mais eficazes contra a espionagem. Isso porque, conforme denunciou o ex-analista de inteligência americana Edward Joseph Snowden, que tornou público detalhes de vários programas altamente confidenciais de vigilância eletrônica dos governos de Estados Unidos e Reino Unido, a vigilância massiva de dados eletrônicos não é possível sem a colaboração de empresas de telecomunicação. São elas que detêm imensos bancos de dados, e que deveriam protegê-los. Uma lei que pudesse impedi-las terminantemente de repassar informações aos órgãos de inteligência brasileiros ou estrangeiros, com punições duras, poderia inibir a prática.

Segundo Marcel Leonardi, em texto publicado na Revista do Advogado (2012, p. 112):

> O modelo adotado pelo Marco Civil da Internet contempla adequadamente todos os participantes do ecossistema on-line. O texto atual do projeto de lei assegura a proteção da rede, fomenta a inovação on-line e protege os direitos dos usuários, sempre com observância do devido processo legal, e, com isso, estabelece a imprescindível segurança jurídica necessária para o crescimento da economia digital e da internet no Brasil. Por esses motivos, pensamos que o Marco Civil da Internet é um bom exemplo do melhor caminho a seguir quando se pensa em regulação da internet.

O famigerado Marco Civil da Internet, assim que aprovado, apesar de já se encontrar um tanto quanto defasado, certamente irá ser um modelo em termos de legislação no campo virtual, e deverá propor mudanças radicais positivas na utilização da rede mundial de computadores.

8 CONCLUSÃO

Este trabalho não tem a finalidade de esgotar os assuntos então apresentados, porém, apenas dar uma ideia do que está ocorrendo ante as mudanças apresentadas.

De acordo com a Constituição da República Federativa do Brasil de 1988, em seu artigo 5º, podemos encontrar a palavra intimidade em dois incisos:

> 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: (...)
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;

Tais dispositivos não são os únicos que garantem referidos direitos, porém, são os principais encontrados em nossa constituição federal.

Com o advento de leis específicas, em especial a Lei nº 12.737 de 2012, nosso país está se inserindo, tardiamente, na lista de países que já apenam crimes relacionados ao mundo cibernético.

Um exemplo do supra mencionado é que, atualmente, mais de uma centena de países contam com leis que protegem os dados pessoais. Números apenas da América Latina, dão conta que Paraguai, Peru, Argentina, Colômbia e Uruguai já aprovaram leis que garantem a privacidade de dados dos seus usuários.

Há que se falar também que o Marco Civil da Internet proporcionará grandes e importantes inovações na proteção dos usuários na rede mundial de computadores, proteção que, atualmente, não encontra o devido suporte legal.

As mudanças e alterações ocorridas, apesar de tardias, irão dar guarida a um número de nacionais que somente cresce com o acesso facilitado da

banda larga. Com o caos do trânsito das grandes e médias cidades, e também com a violência sem precedentes, os consumidores irão dar preferência às compras virtuais, que, para isso, terão de confiar cada vez mais seus dados aos sites especializados em vendas.

O desenvolvimento de qualquer nação soberana, hodiernamente, depende de um plano tecnológico sério e de ponta para suportar a demanda que está por vir. Não podemos mais sermos vítimas de ataques de outras nações, como a que ocorreu no ano passado com os Estados Unidos da América, em um episódio que gerou enorme desconforto entre esses dois Estados, muito menos sermos atacados pelos nossos infratores nacionais.

Não podemos esquecer também que a pedra fundamental para que não se ocorra invasões ou mesmo ataques cibernéticos variados é a simples e eficaz educação. Não basta possuirmos as ferramentas mais modernas e avançadas do mundo, sem que as pessoas que acessam tais máquinas continuem na idade da pedra no quesito intelectual e moral.

Sem sombra de dúvidas, o aperfeiçoamento integral de todas as faculdades humanas, é o ponto central do desenvolvimento de uma sociedade livre e justa. O avanço tecnológico é mais um degrau no desenvolvimento humano, não podendo andar apartado da educação e do respeito.

Com a edição de leis e a efetiva punição dos infratores no campo virtual, haverá, ao menos, uma intimidação maior ante tais delitos.

Somente com dispositivos legais atuais e eficientes, e com o investimento no desenvolvimento da educação nacional, é que poderemos tentar brecar esse novo tipo delituoso chamado de crime virtual.

9 REFERÊNCIAS

BLUM, Renato M.S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. **Manual de Direito Eletrônico e Internet.** São Paulo: Lex Editora, 2006.

BOCCHINI, Lino. **Quem é o culpado pelo suicídio da garota em Veranópolis?** Disponível em: <http://www.cartacapital.com.br/blogs/blog-do-lino/o-suicidio-da-adolescente-de-veranopolis-e-nossa-culpa-6036.html>. Acesso: em 19 dez. 2013.

BRASIL. **Código Penal, Código de Processo Penal, Constituição Federal, Legislação Penal e Processual Penal**. 14ª. ed. São Paulo: Editora Revista dos Tribunais, 2012.

BRASIL. Lei nº. 12.737, de 30 de novembro de 2012. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**. Brasília, DF, 16 jul. 1990. Disponível em:

<http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 20 dez. 2013.

BRASIL. Lei nº. 8.069, de 13 de julho de 1990. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**. Brasília, DF, 03 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 dez. 2013.

BRASIL. Lei nº. 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. **Diário Oficial da União**. Brasília, DF, 03 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 20 dez. 2013.

BRASIL. Supremo Tribunal de Justiça. Processual Penal 628. ADI 855-2. Tribunal de Justiça do Distrito Federal. Disponível em: <http://stj.jusbrasil.com.br/jurisprudencia/21063887/acao-penal-apn-628-df-2010-0042090-3-stj/inteiro-teor-21063888>. Acesso em: 15 de dez. 2013.

BRASIL. Projeto de Lei nº. 2126/2011, de 24 de agosto de 2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 24 ago. 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 20 dez. 2013.

BRASIL. Lei nº. 5.250/1967, de 10 de fevereiro de 1967. Regula a liberdade de manifestação do pensamento e de informação. Brasília, DF, 9 fev. 1967. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l5250.htm>. Acesso em: 20 dez. 2013.

BRASIL. Tribunal de Justiça. Recurso em Sentido Estrito n. 0015931-17.2008.8.26.0114. Tribunal de Justiça do Estado de São Paulo. Disponível em:

<http://esaj.tjsp.jus.br/cpo/sg/search.do?paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=0015931-17.2008&foroNumeroUnificado=0114&dePesquisaNuUnificado=0015931-17.2008.8.26.0114&dePesquisa=&pbEnviar=Pesquisar>. Acesso em: 15 de dez. 2013.

BRASIL. Tribunal de Justiça. Ação Penal Privada n. 0195240-78.2010.8.26.0000. Tribunal de Justiça do Estado de São Paulo. Disponível em:

<http://esaj.tjsp.jus.br/cpo/sg/search.do?paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=0195240-78.2010&foroNumeroUnificado=0000&dePesquisaNuUnificado=0195240-78.2010.8.26.0000&dePesquisa=&pbEnviar=Pesquisar>. Acesso em: 15 de dez. 2013.

BRASIL, Banco do. Segurança. Disponível em:

<http://www.bb.com.br/portalbb/page3,105,5212,0,0,1,1.bb?codigoNoticia=2976&codigoRet=579&bread=1&codigoMenu=565>. Acesso: em 21 dez. 2013.

BREDA, Tadeu. **Apenas soluções técnicas não podem conter espionagem na internet**. Disponível em: <http://www.redebrasilatual.com.br/saude/2013/07/apenas-solucoes-tecnicas-nao-podem-conter-espionagem-pela-internet-8210.html>. Acesso: em 21 dez. 2013.

CAPEZ, Fernando. **Curso de Direito Penal – Parte Geral 1**. 16ª. ed. São Paulo: Saraiva, 2012.

CAPEZ, Fernando. **Direito Penal Simplificado – Parte Especial**. 16ª. ed. São Paulo: Saraiva, 2012.

CASTILHO, Wanderson. **Manual do Detetive Virtual.** 2ª. ed. São Paulo: Editora Urbana, 2012.

CASTRO, André Zanatta Fernandes de; SIVIERO, Fabiana Regina. **Privacidade na era da evolução digital.** Revista do Advogado. Nº 115. Ano XXXII, p. 55/56, abril de 2012.

CONCEITOS Iniciais da Internet. Disponível em: <http://brgiga.com/index.php?p=subcont&id=8>. Acesso: em 20 dez. 2013.

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

CONGO, Mariana. **Lei Carolina Dieckmann e Lei Azeredo entram em vigor hoje; saiba onde denunciar**. Disponível em: <http://blogs.estadao.com.br/radar-tecnologico/2013/04/02/lei-carolina-dieckmann-e-lei-azeredo-entram-em-vigor-hoje-saiba-onde-denunciar/>. Acesso: em 05 jan. 2014.

CRIMES PRATICADOS NA INTERNET. Disponível em:

<http://leiout.com.br/post/5601736444/crimes-cometidos-atraves-da-internet>. Acesso: em 20 dez. 2013.

DADOS da proprietária do veículo que abandonou o cão à própria sorte numa avenida em São Paulo. Disponível em: <http://www.anonymousbrasil.com/dossies/dados-da-proprietaria-veiculo-que-abandonou-o-cao/>. Acesso: em 20 dez. 2013.

DAOUN, Alexandre Jean e BLUM, Renato M. S. Opice. "**Cybercrimes", in Direito & Internet**. São Paulo: Edipro, 2000.

EXAME. **Edward Snowden teme por sua vida, segundo advogado russo**. Disponível em: <http://exame.abril.com.br/mundo/noticias/edward-snowden-teme-por-sua-vida-segundo-advogado-russo>. Acesso: em 21 dez. 2013.

GAMA, Remy. **Crimes da Informática**. Disponível em:

<http://www.cesarkallas.net/arquivos/livros/direito/00715%20-%20Crimes%20da%20Inform%E1tica.pdf>. Acesso: em 10 jan. 2014.

GOMES, Luiz Flávio Gomes. **A (in)eficácia da Lei Carolina Dieckmann**. Disponível em: <http://m.congressoemfoco.uol.com.br/noticias/a-ineficacia-da-lei-carolina-dieckmann/>. Acesso: em 21 dez. 2013.

GROSSMAN, Luiz Osvaldo. **Brasil tem mais de 83 milhões de internautas, segundo IBGE**. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=35001&sid=14#.Utz7nRBTvIV>. Acesso: em 21 dez. 2013.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet.** 2ª. ed. São Paulo: Editora Juarez de Oliveira, 2009.

KAMINSKI, Omar. **Internet Legal – o direito na tecnologia da informação**. 1ª. ed. Curitiba: Juruá, 2009.

KARASINSKI, Lucas. **Como a internet passa de um continente para outro**. Disponível em: <http://www.tecmundo.com.br/internet/31311-como-a-internet-passa-de-um-continente-para-o-outro-.htm#ixzz2gNQ9ZyLQ>. Acesso: em 21 dez. 2013.

LEONARDI, Marcel. **Internet e regulação: o bom exemplo do Marco Civil da Internet.** Revista do Advogado. Nº 115. Ano XXXII, p. 99/113, abril de 2012.

MARCO CIVIL da Internet. **Marco Civil**. Disponível em: <http://marcocivil.org.br/>. Acesso: em 21 dez. 2013.

MELLO FILHO, Paschoal Mauro Braga. **Crimes eletrônicos: Os Perigos do Mundo Digital**. Revista De Villegagnon. ANO II – Nº 2 – 2007. Disponível em: <http://www.mar.mil.br/en/revistaen2007.pdf>. Acesso: em 22 dez. 2013.

MICROSOFT. **O que é malware?**. Disponível em: <http://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx>. Acesso: em 21 jan. 2014.

MULLER, Nicolas. **O começo da internet no Brasil**. Disponível em: <http://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil>. Acesso: em 21 dez. 2013.

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

OLIVEIRA, Adrielson. **A sociedade do conhecimento e a internet**. Disponível em: <http://www.artigonal.com/tecnologias-artigos/a-sociedade-do-conhecimento-e-a-internet-1956537.html>. Acesso: em 21 dez. 2013.

O BRASILEIRO QUER SE CONECTAR. Disponível em: <http://www.midiaindependente.org/pt/blue/2011/09/496930.shtml>. Acesso: em 20 dez. 2013.

OLIVEIRA, Luiz Gustavo Caratti de. **Responsabilidade civil dos bancos nos casos de fraudes pela internet que lesam as contas de seus clientes**. Disponível em:<http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10225>. Acesso: em 21 dez. 2013.

ON LINE FRAUD. Disponível em: <http://www.emc.com/collateral/fraud-report/11802-online-fraud-report.pdf>. Acesso: em 20 dez. 2013.

PERCILA, Eliene. **Skinheads**. Disponível em:

<http://www.brasilescola.com/sociologia/skinheads.htm>. Acesso: em 24 dez. 2013.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** 1ª. ed. Curitiba: Juruá, 2006.

NOVO DICIONÁRIO ELETRÔNICO AURÉLIO, 2004. Novo Dicionário Eletrônico Aurélio versão 5.11a. Positivo Informática LTDA. 1 CD ROM.

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012**. Disponível em:

<http://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012>. Acesso: em 21 dez. 2013.

SANTIAGO, Emerson. **Criptografia**. Disponível em:

<http://www.infoescola.com/informatica/criptografia>. Acesso: em 24 dez. 2013.

SENHA BLOQUEADA NO INTERNET BANKING. Disponível em:

< http://www.reclameaqui.com.br/5466618/banco-do-brasil-s-a/senha-bloqueada-no-internet-banking>. Acesso: em 24 dez. 2013.

SURGIMENTO DA INTERNET. Disponível em:

<http://marketingfuturo.com/surgimento-da-internet>. Acesso: em 23 dez. 2013.

UCHOA, Pablo**. Para especialista americano, espionagem do Brasil não se compara à da NSA.** Disponível em :
<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=35001&sid=14#.Utz7nRBTvIV>. Acesso: em 21 dez. 2013.

DUMAS, Véronique. **A origem da internet**. Disponível em:

<http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html>. Acesso: em 24 dez. 2013.