SPENCER TOTH SYDOW

***DELITOS INFORMÁTICOS PRÓPRIOS: UMA ABORDAGEM
SOB A PERSPECTIVA VITIMODOGMÁTICA.***

Dissertação apresentada junto à Egrégia Faculdade de Direito da Universidade São Paulo, ao Departamento de Direito Penal, Medicina Forense e Criminologia, sob orientação do Prof. Dr. Sergio Salomão Shecaira, como exigência parcial para a obtenção do título de mestre.

**FACULDADE DE DIREITO DO LARGO SÃO FRANCISCO – UNIVERSIDADE DE
SÃO PAULO (USP)**

São Paulo – 2009

BANCA EXAMINADORA

RESUMO

O trabalho trata da abordagem da delinquência frente à sociedade informática e dos riscos trazidos pelas tecnologias, estimuladoras da prática do delito por conta de suas características especiais. Tal análise concluirá que as condutas praticadas na nova realidade apontam para a necessidade de adaptação do Direito Penal pela criação de novos valores e, então, novo bem jurídico a ser protegido. Em seguida, frente aos principais delitos tipificados nos ordenamentos jurídicos, será apresentada a vitimodogmática que servirá de instrumento para uma interpretação das figuras penais sob a ótica de sua gênese e a contribuição que a vítima tem em tal processo.

ABSTRACT

This study is about the delinquency considering the informatic society and the risks posed by technology, stimulating crime occurrence due to its special characteristics. This analysis concludes that the conduct charged in new environment points to the need of reorganizing criminal law through the creation of new values and new rights to be protected. Therefore, facing the main crime concerns in legal systems, the victimodogmatic will be presented as an instrument for the interpretation of criminal figures from the perspective of its genesis and the contribution that the victim has in this process.

ÍNDICE

Agradecimentos	08
Nota Introdutória	09
Uma Declaração de Independência do Ciberespaço	10
1. Introdução	12
2. A Sociedade de Risco Informática	21
3. Os Delitos Informáticos	45
Aspectos Preliminares	45
Os Três Elementos da Segurança Informática	58
Confidencialidade	59
Integridade	61
Disponibilidade	63
Um Novo Bem Jurídico	64
Uma Nova Definição de Delito Informático	75
Características do Direito Informático	76
Interatividade	76
Mobilidade (ou Portabilidade)	78
Conversabilidade	79
Conectividade	80
Mundialização	81
Fracionabilidade	83
Divisibilidade	84
Intangibilidade	87
Disponibilidade	90
Pluralidade	92
Ubiquidade (ou Simultaneidade)	93

Anonimidade	96
Velocidade	98
Principais Delitos Informáticos Próprios Tipificados	99
Instrusão Informática	101
“Furto” de Identidade	103
Inserção de Código Malicioso	108
<i>Scamming</i>	110
<i>Spamming</i>	114
Interceptação de <i>Email</i>	118
A Criminologia e a Difícil Prevenção do Delinquente Informático	120
O Autor do Crime Informático	125
4. Vitimologia e Vitimodogmática	132
A Parelha Vítima-Vitimário	155
A Precipitação Vitimal	158
Perigosidade Vitimal	159
Receptividade Vitimal	159
A Prevenção Vitimal	160
Abordagem Vitimodogmática dos Delitos Informáticos Próprios Puros	164
A vítima solitária	166
A vítima ignorante	172
A vítima idosa	176
A vítima criança/adolescente	178
A vítima gananciosa	182
A vítima curiosa	186
As Vítimas Frente aos Delitos Informáticos	189
A Vítima da Intrusão Informática	190
A Vítima da Contaminação por Código Malicioso	194

A Vítima da Violação de <i>Email</i>	197
A Vítima do Dano Informático	199
A Vítima do <i>Scamming</i>	202
A Vítima do <i>Spamming</i>	207
5. As Consequências da Atitude da Vítima	210
Consentimento do Ofendido	214
Autocolocação da Vítima em Risco	218
A Vítimodogmática e suas Implicações na Conduta Delinquente	225
Uma Proposta para Delitos Informáticos	226
A Vítima na Política Criminal de Combate à Delinquência Informática	236
6. Conclusão	246
Glossário	250
Bibliografia	261

AGRADECIMENTOS

Ao admirado orientador e amigo, Professor Doutor Sérgio Salomão Shecaira, por ter acreditado em mim e ajudado muito a superar todas as dificuldades. Pelas contribuições brilhantes e sempre pertinentes, pelo apoio e pela força que sempre demonstra.

Aos meus pais Spencer e Barbara, ao meu lado em todos os momentos, ensinando, estimulando, encantando e fazendo cada dia valer a pena.

À minha irmã Cristina, pelo entusiasmo e por ter sido responsável pelo começo de tudo.

Ao meu irmão Thomas, pela força e companherismo, pelas filosofias e conversas e pela infinita cumplicidade.

À minha pequena Marcelle, pelo apoio, pela compreensão e pelo colorido que dá à vida.

A meus amigos da Univerisdade de São Paulo por tudo o que me ensinaram, em especial aos Professores Renato de Mello Jorge Silveira, Guilherme de Souza Nucci, Alamiro Velludo Salvador Neto, Luciano Anderson de Souza e ao saudoso Antonio Luiz Chaves Camargo (*in memoriam*).

À Dalva Veramundo Bizerra de Souza, secretária do departamento de Direito Penal, Medicina Forense e Criminologia, pelo carinho, presteza e gentileza.

Aos amigos Cavaleiros, sempre.

Aos meus cães, pela companhia perpétua.

NOTA INTRODUTÓRIA

O presente trabalho trata da Delinquencia Informática. Por ser um tema bastante específico, exigirá do leitor alguns conhecimentos na área de informática e tecnologia, além da familiaridade com termos utilizados rotineiramente na língua inglesa. Para facilitar a compreensão, sempre que possível desenvolvemos explicações paralelas em notas de rodapé para auxiliar na compreensão de especificidades técnicas de alguma relevância na compreensão do assunto em pauta.

Também, devido ao fato de o tema ter ainda modesto desenvolvimento na doutrina pátria mas amplo desenvolvimento em países de língua inglesa, diversos autores citados no desenvolvimento do trabalho podem não ser familiares a nossos bancos acadêmicos porquanto oriundos de países em que vigora o sistema da *common law*, de direito consuetudinário, portanto. Porém, todas as referências citadas possuem renome no cenário da criminologia internacional ou nos estudos dos delitos informáticos em suas respectivas universidades.

Houve também bastante apoio em textos, artigos e *papers* disponíveis na rede mundial de computadores e que no mais das vezes são citadas nos rodapés das páginas. Optou-se por acrescentar sempre, além da data de acesso, também o horário preciso, tendo-se em vista a grande volatilidade de alguns materiais no meio eletrônico.

As citações no corpo do texto foram todas traduzidas para a língua portuguesa, mantendo sempre, em notas, a transcrição do original para conferência do leitor, buscando levar maior fluidez à leitura.

Por fim, destaca-se, ao final do trabalho, um glossário constituído para referência técnica mais precisa das expressões utilizadas.

UMA DECLARAÇÃO DE INDEPENDÊNCIA DO CIBERESPAÇO¹

Por John Perry Barlow²

“Governos do Mundo Industrial, vocês são gigantes de ferro e aço. Eu venho do Ciberespaço, a nova casa da Mente. Em prol do futuro eu peço a vocês que nos deixem em paz. Vocês não são bem vindos entre nós. Vocês não têm domínio onde nós nos reunimos.

Não temos governo eleito e nem estamos dispostos a ter um, então dirijo-me a vocês com a mesma autoridade do que aquela que fala por si só na liberdade. Eu declaro o espaço global social que estamos construindo a ser naturalmente independente de tiranias que procurem impor-se sobre nós. Vocês não têm direito moral de nos reger nem de possuir nenhum tipo de medida de força de que tenhamos qualquer medo.

Os governos derivam seus poderes do consentimento dos governados. Vocês não foram chamados e nem receberam nossos consentimentos. Nós não os convidamos. Vocês não nos conhecem e nem conhecem nosso mundo. O Ciberespaço não jaz em suas fronteiras. Não acreditem que vocês podem construí-lo como fizeram em projetos públicos de construção. Vocês não podem. É um ato natural e ele cresce através de ações coletivas.

Vocês não comprometem nossa grandiosa e unida conversação nem criam a riqueza de nossos mercados. Vocês não conhecem nossa cultura, nossa ética ou as nossas regras não escritas que já regulam nossa sociedade de forma melhor do que com qualquer de suas imposições.

Vocês clamam haver problemas entre nós que demandam soluções de vocês. Vocês

¹ Disponível em <http://homes.eff.org/~barlow/Declaration-Final.html> (versão em inglês) ou em <http://www.dhnet.org.br/ciber/textos/barlow.htm> (versão em português). Ambos acessos em 23.12.08 às 11:44hs

² John Perry Barlow, nascido em 3 de outubro de 1947 é poeta norte americano, palestrante, ativista político, co-fundador da Electric Frontier Foundation, conhecido por ser um ciberlibertariano. O libertarianismo é a filosofia ou sistema de crença que dá prioridade à liberdade individual. Pode ser associada com o libertarismo clássico relacionado com assuntos econômicos ou de proteção às liberdades negadas que declaram o direito de indivíduo existir livre das interferências do Estado ou da comunidade, exceto no que se refere às ações do indivíduo que constituam prejuízo a outros. (“A philosophy or belief system which gives priority to the liberty of the individual. May be associated with classical liberalism regarding economic matters or the protection of those negative liberties which declare the right of the individual to be free from interference by the state, or the community, unless the actions of the individual constitute harm to others”). Online Dictionary of Social Science. Disponível em <http://bitbucket.icaap.org/dict.pl?alpha=L>. Acesso em 05.01.09 às 14:47hs.

usam tal clamor para invadir nosso recinto. Muitos desses problemas não existem. Onde estiverem os verdadeiros conflitos e os verdadeiros erros, nós identificaremos e resolveremos da nossa forma. Estamos formando nosso próprio Contrato Social. Este governo irá crescer de acordo com nosso mundo e não o de vocês. Nosso mundo é diferente.

O Ciberespaço consiste em transações, relacionamentos e foi concebido como uma nova estrutura comunicativa. Nosso mundo está ao mesmo tempo em todos os lugares e em nenhum, e ninguém pode viver nele.

Estamos criando um mundo em que qualquer um pode ingressar sem qualquer privilégio ou preconceito quanto à raça, poder econômico, força militar ou condição de nascimento.

Estamos criando um mundo em que qualquer um, em qualquer lugar, pode expressar suas crenças, não importa quanto singular, sem medo de ser coagido ao silêncio ou ao conformismo.

Seus conceitos de propriedade, expressão, identidade, movimento e o contexto não se aplicam a nós. Eles são baseados no conceito de matéria e não há matéria aqui.

Nossas identidades não têm corpo, então, diferentemente de vocês, nós não podemos ser coagidos por forças físicas. Acreditamos que pela ética, iluminado interesse próprio e bem estar, nossa governança irá emergir. Nossas identidades poderão estar distribuídas por muitas de suas jurisdições. A única lei que nossa cultura constituinte reconhece é a Lei de Ouro. Acreditamos que seremos capazes de criar nossas próprias soluções com essa base. Nós não aceitamos soluções que vocês tentam nos impor.

(...)

Nós criaremos a civilização da Mente no Ciberespaço. Que nós consigamos fazê-la mais humana e justa do que o mundo que seus governantes fizeram antes.”

Davos, Suíça

8 de fevereiro de 1996

INTRODUÇÃO

De tempos em tempos, a sociedade sofre revoluções que a transformam. Exemplificativamente, assim foi com as Revoluções Burguesas, mais especialmente a Revolução Francesa que por conta do questionamento trouxe o início da positivação de direitos fundamentais. Assim foi com a Revolução Industrial que por conta dos avanços tecnológicos trouxe a substituição das ferramentas pelas máquinas, consolidando o capitalismo como modo de produção.

Contudo, com os avanços trazidos pelas revoluções, há também problemas e sacrifícios. A Revolução Francesa trouxe morte e fragilização dos Estados. A Revolução Industrial trouxe desemprego e exploração desproporcional da mão de obra trabalhadora.

Em tempos recentes³ surgiu uma nova Revolução, por nós denominada Revolução Digital⁴. Entende-se por Revolução Digital o movimento de inserção na sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano cidadão progride. A popularização do computador por conta de seu barateamento e melhor acessibilidade contribui para que a cada dia mais pessoas ao largo do planeta tenham acesso à informática e, conseqüentemente, à rede mundial de computadores.

Conforme evolui o conhecimento humano, juntamente a sociedade tem a seu dispor ferramentas que facilitam sua vida. A capacidade intelectual humana faz com que as ciências tomem importante papel, melhorando a forma como os homens interagem e permitindo que se aproveite melhor os recursos, dentre eles o tempo. Exemplificativamente, regressemos 50 anos na história e a ciência era incapaz de prever catástrofes climáticas com a precisão que hoje trazem os satélites; regressemos 30 anos e exames como a tomografia eram inconcebíveis, levando doentes a diagnósticos tardios ou imprecisos; regressemos 5 anos e tecnologias sem

³ No final da década de 1960 surgiu a ARPANET, rede militar de computadores desenvolvida pelos Estados Unidos da América do Norte, embrião da atual rede mundial de computadores popularmente conhecida como Internet. A crescente popularização da rede mundial dá mostras de que a revolução ainda está em andamento, conforme ocorre a popularização da rede.

⁴ Também denominada “Virada Cibernética” pelo sociólogo Laymert Garcia dos Santos, em *Revolução tecnológica, Internet e socialismo* / Laymert Garcia dos Santos... [et. al.]. – São Paulo : Editora Fundação Perseu Abramo, 2003. p.9.

fio eram perspectivas ideais.

Em suma, conforme a tecnologia vai tomando espaço na vida do cidadão, torna-se fundamental que o indivíduo passe a ter certo conhecimento pressuposto para poder lidar com as modernidades. Certamente, grandes desenvolvimentos trazem consigo novas responsabilidades e novos riscos. A existência de satélites no espaço pressupõe novos estudos, gastos altos com manutenção e dificuldades operacionais maiores, assim como novos procedimentos com matérias radioativas ou ondas de rádio descontroladas requerem diligências maiores por conta de sua capacidade de transformação celular ainda parcialmente desconhecida.

No mesmo seio, o evoluir social trouxe a tecnologia para o cotidiano das pessoas. A informática⁵ passou a ser ramo independente de estudo tecnológico, exclusivo e imprescindível para o cidadão que, inclusive, dedica-se a cursos para aprender a manusear o computador e seus *softwares*. Todo o esforço dos indivíduos para dominar parte desse conhecimento se dá pelo fato de que a computação veio como ferramenta facilitadora das tarefas domésticas e laborativas: elaborar planilhas, gráficos, lista de compras, escrever textos, conversar a distância, fazer pagamentos, deveres de casa, dentre tantas outras possibilidades, são exemplos de atos favorecidos e facilitados pelo surgimento dos computadores.

O avanço e popularização da tecnologia aliada à informática fizeram com que surgissem novos hábitos e, com eles, novos valores. Na medida em que tais valores adquirem relevância social e econômica, surgem também problemas quanto à sua preservação.

A computação, todavia, não parou de se desenvolver no aspecto individual. Paralelamente, surgiu a Internet, uma rede virtual⁶ em que um usuário se conecta para ter acesso a uma ampla gama de computadores interligados, dispondo de dados para consulta e utilização por qualquer um que consiga acessar através de mecanismos e linguagem próprios. A rede passou a ser um ambiente de intercomunicação (mediata ou imediata), de

⁵ Aqui referido como processo de tratamento automático da informação por meio de computadores.

⁶ “Redes são estruturas abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação (por exemplo, valores ou objetivos de desempenho). Uma estrutura social com base em redes é um sistema aberto altamente dinâmico de inovação sem ameaças ao seu equilíbrio.” CASTELLS, Manuel. *Sociedade em Rede*. Vol. I. Paz e Terra, São Paulo, 1999, p. 499.

relacionamento, de pesquisa, de troca de informações, programas, arquivos multimídia, de divulgação de produtos, de autopromoção, enfim, uma verdadeira ferramenta de comunicação, interação, criação, transformação e busca, e que, por trazer avanços, traz consigo toda a necessidade de novo aprendizado.

Novos conceitos passaram a existir com a tecnologia. Enquanto que a maioria dos bens antigamente eram representados por átomos, hoje boa parte deles é representada por *bits*. Os átomos formam a substância tangível, enquanto que os *bits* compõem a linguagem (intangível) utilizada pela informática para compor os arquivos, programas e sinais de comunicação. Enquanto que no passado era necessário tinta, papel, cola, selo, envelope e correios para se comunicar (todos elementos tangíveis), hoje, para o envio de uma mensagem eletrônica basta que cada indivíduo digite em seu teclado a mensagem e clique em enviar.

A tecnologia fez com que prescindíssemos de uma boa gama de elementos materiais, levando, pois, a uma ruptura de valores da sociedade e à criação de outros. Os correios hoje perderam parte de seu significado, de sua função inicial. Em alguns estabelecimentos de ensino, cadernos e canetas também deixaram de existir, uma vez que o aluno toma nota da matéria diretamente em seu fichário de um disco rígido. O pagamento via cartão de crédito ou de débito também mostra que dinheiro, hoje, é uma representação feita por *bits* nos sistemas bancários.

Conjuntamente à praticidade trazida pela tecnologia, vieram também os sacrifícios a ela aliados. O ser humano aumentou seu tempo sozinho, relacionando-se e comunicando-se virtualmente, precipuamente diante de uma tela. A presença física (átomos) foi substituída pela “presença virtual”, em que computadores se comunicam, sob administração de seus usuarios. Protegidos pelas telas, pessoas físicas passam a representar usuarios anônimos num universo virtual sem fronteiras. Bens compostos por *bits*, também, passam a existir e ser atingidos, graças às novas tecnologias. Segredos industriais, direitos autorais, dinheiro, bancos de dados entre tantos outros valores passam a existir na forma imaterial.

Como resposta à Revolução Digital, mostrou-se o ambiente eletrônico permeado por falhas e constantemente sujeito a ataques por conta de brechas de programação, falhas de segurança, técnicas de sobrepujamento, engenhosidade social e até mesmo inventividade de

sujeitos por vezes mal intencionados, por vezes simplesmente visando superar desafios.

A reação da sociedade para tais atos, verificando-se a ordem de prejuízos causados, foi a de manifestar reivindicação acerca da necessidade de se estabelecer a relevância dos novos bens jurídicos criados pela informática (segurança informática, dados, etc) e punir a violação a tais valores. O Brasil no quesito legislativo, contudo, permanece bastante atrasado.

Assim, criado estava o Direito Penal Informático, que passou a estudar a nova criminalidade bem como buscar formas para sua prevenção. Universidades, inclusive, criam cadeiras para dedicar estudiosos ao tema diuturna e exclusivamente⁷.

O tema escolhido é uma mescla da tal criminalidade do futuro com o fato de que os usuarios, parques conhecedores da sociedade – denominada de risco – em que navegam, acabam por serem grandes incentivadores (omissos por vezes – co-causadores) de atitudes ilícitas.

A maior parte das vítimas do delito informático são cidadãos comuns que em geral não compreendem corretamente o meio em que estão e nem as dificuldades e os prejuízos que podem lhes ser impingidos através da eletrônica, por outro usuario.

Por conta de o meio informático trazer sensações como a de segurança, afastamento, anonimidade e frieza, e por conta de situações pessoais do usuario-vítima, a rede mundial de computadores e outros meios eletrônicos acabam ocasionalmente sendo utilizados de forma irresponsável e impulsiva.

O desenvolvimento de novos valores com relevância econômica e social é explícito com a difusão exponencial da informática pelo mundo. O ser humano cada vez mais é dependente da informática para suas tarefas cotidianas de comunicação, pagamento de contas, entretenimento, telefonemas, etc.

Por certo há lacunas na parte geral e especial do Direito Penal Brasileiro que merecem maior atenção legislativa e também mais detido estudo para se compreender melhor o universo

⁷ Um bom exemplo está na Universidade de Leeds, na Inglaterra, que criou a cadeira de ciberdireito, dedicada exclusivamente ao estudo dos impactos das tecnologias da informação nos sistemas legais. <http://www.law.leeds.ac.uk/LeedsLaw/GenericPage.aspx?ID=89&TabID=4&MenuID=40&SubMenuID=54>.

tratado. Há tipos demandados pela nova doutrina que necessitam ser pensados diante da realidade informática brasileira para que a interpretação do Direito Penal não se torne falha, passando sensação de impotência estatal e impunidade aos agentes.

O Direito Informático – e o Direito Penal Informático por consequência – é área ainda pouco explorada, pouco estudada e a que somente alguns pensadores dedicaram seu tempo. A língua estrangeira e a necessidade de um entendimento técnico em informática são alguns entraves que levam quando muito a elaboração de artigos, *papers* e vez ou outra pareceres e sentenças originais. Muito comum os estudos do tema serem feitos paralelamente a um caso de algum país evoluído, em que vigem letras penais diferentes e, por vezes, até classificações constitucionais bastante diversas.

Em suma, ainda há pouca originalidade doutrinária em nosso país quanto ao tema aliada a limites legislativos e pouca compreensão de teorias modernas do crime que permitiriam avanços nos estudos da criminalidade eletrônica.

O evoluir das teorias do delito no Direito Penal Brasileiro parece deixar algumas dúvidas no que se refere à forma como o comportamento da vítima se aplicaria em casos concretos. Há também o fato de que não buscou o legislador, em geral, frente à doutrina estrangeira mais moderna, adequar seus projetos para reformar o Código Penal conforme os novos raciocínios sobre risco trazidos pelo funcionalismo positivado da Europa.

A doutrina brasileira, contudo, busca esforçar-se para conhecer e entender as novas teorias, inclusive apreciando os crimes já existentes, via de regra com base na legislação ultrapassada em muitos aspectos e necessitando de atualização. Os delitos informáticos, contudo, por serem recentes, ainda permanecem atrás de um véu de incompreensão.

A realidade eletrônica é pouco difundida em nosso ambiente. Enquanto que aproximadamente 70% dos norte-americanos⁸ têm acesso à tecnologia, o Brasil ainda engatinha no processo de cultura informática: os programas de computador e peças vêm

Acesso em 12.12.08 às 17:11hs.

⁸ De acordo com o IBGE, em 2007 os EUA registraram população de 305.826.000 habitantes. O site Internet World Statistics (<http://www.Internetworldstats.com/top20.htm>) calculou que em Julho de 2007, 211 milhões de norte americanos eram usuarios da rede. O cruzamento das informações levaria a um percentual de cerca de 70% da população norte-americana com acesso à rede mundial de computadores .

excessivamente onerosos para o país, dificultando o acesso da população já usuária aos novos avanços tecnológicos⁹, além de incentivar a pirataria¹⁰.

Curioso notar que apesar de o Brasil ser pouco desenvolvido no tocante à popularização informática, os dez grupos de *crackers* mais ativos do mundo estão aqui, demonstrando que nosso país possui um avançadíssimo potencial para o ciberdelito. Some-se a isso o fato de que em 2002, o Brasil figurou como o 2º país do mundo¹¹ vítima de ataques cibernéticos, somente atrás dos EUA.

Estranhamente, há pouco estudo do tema no país e poucos projetos de lei¹² (muitos de aplicabilidade duvidosa) em trâmite no Congresso Nacional acerca do Direito Penal Informático, de certa forma levando o país a uma condição de “*paraíso do ciberdelito*”.

A criação de um estudo profundo de todo o Direito Penal enviesado para o *ciberdelito* é necessário para a compreensão da nova criminalidade. É importante que os operadores do direito compreendam melhor as particularidades da parte geral e especial do Código Penal – e muito especialmente suas falhas na punição e repressão dessa modalidade de delito – para que se iniciem frentes de contenção desta modalidade criminosa, aprovações de bons projetos e para que as dúvidas hoje existentes possam ser sanadas.

O Princípio da legalidade é uma garantia penal intransponível no país. Os magistrados são sabidamente submetidos à lei penal, obrigados a absolver quando em dúvidas e proibidos

⁹ De acordo com o IBGE, em 2007 o Brasil registrou população de 191.791.000 habitantes. O site Internet World Statistics (<http://www.Internetworldstats.com/stats15.htm>) calculou que em Dezembro de 2007, 42,6 milhões de brasileiros eram usuarios da rede. O cruzamento das informações levaria a um percentual de cerca de 22% da população brasileira com acesso à rede mundial de computadores. Entretanto, Pesquisa Ibope NetRating mostra que o número de usuarios brasileiros está na marca de 22 milhões. Fonte: <http://idgnow.uol.com.br/Internet/2008/03/26/numero-de-internautas-residenciais-chega-a-22-milhoes-no-brasil/>. Acesso em 08.06.2008 às 18:06hs.

¹⁰ Aqui cabe citarmos a ideia de “exclusão digital” difundida pelo mundo pela expressão “digital divide”, e que representa a ideia de que há, em toda a sociedade, parcela que sequer consegue acesso a tecnologias, gerando imediatamente destaque no conceito de falta de iguais oportunidades a todos os cidadãos.

¹¹ “Brasileiros lideram Ranking Mundial de Hackers” - artigo disponível no site: http://www.bbc.co.uk/portuguese/ciencia/020823_hackerscg.shtml Acesso em 14.08.08 às 18:14hs. Também em “Brasil lidera ranking de ataques a contas bancárias por hackers” em <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=15343&sid=18>. Acesso em 14.08.08 às 12:20hs.

¹² Em pesquisa ao site da Câmara dos Deputados, encontra-se os seguintes projetos de lei sobre o tema em tela: PL-89/2003 (originalmente PL-84/1999), PL-3943/1997 (arquivada), PL-1713/1996 (tramitando em conjunto com PL-1070/1995). No Senado Federal, PLS 76/2000, PLS 152/1991 e PLS 137/2000, além do

de praticar analogias *in malam partem*. Não raro por meio da interpretação paralela se equivalem institutos e figuras para se conseguir penalizar o delito cometido pela eletrônica como, por exemplo, o estelionato. Algumas fórmulas genéricas de tipos penais, porém, nem sempre equivalem ao tipo justo e adequado para um delito cometido pelo meio eletrônico. Algumas qualificadoras existentes hoje não condizem minimamente com o potencial lesivo de um delito desta modalidade; algumas penas chegam a ser medíocres frente ao vulto que toma um *ciberataque* e a ficção do delito continuado beneficia reiteradamente os *cibercriminosos*, vez que a ação é em regra plúrima. Mister avaliar-se todo o enfoque do Direito Penal com esse pensamento.

O tema da dissertação será a demonstração de particularidades do meio eletrônico, com especial atenção à consequência das atitudes vitimais. Certamente boa parte da ênfase estará na rede mundial de computadores (Internet), mas não ficaremos restritos a tal enfoque.

O tema traz maiores desafios para desenvolvimento, em especial pela escassez de doutrina brasileira sobre a nova criminalidade, além de se ressaltar o fato de que tais livros são raramente atualizados frente às tecnologias. Pouquíssimos artigos são redigidos em língua portuguesa e ainda são poucos os pensadores de Direito Penal que se dedicam também a conhecer as novidades da tecnologia e os avanços da informática, sendo capazes de ver a potencialidade lesiva dos novos aparatos e afins. A doutrina ainda sofre para compreender a criminalidade eletrônica, por quase não haver tipos na legislação penal pátria, por não se compreender o perfil e a potencialidade lesiva dos autores, e, como mote desta obra, por não ficar claro o tamanho da responsabilidade e estímulo dado pelas vítimas.

A dificuldades de contenção e prevenção da criminalidade também se justifica por pouco se estudar a etiologia do crime sem se ater com afinco à postura das vítimas diante das ações ilícitas. A incapacidade em se prever as formas de conduta pelo dinamismo tecnológico e o fato de a tecnologia evoluir com velocidade imensa frente ao elefântico pensamento dos tribunais contribui para o atraso.

Somada aos obstáculos para se ler sobre criminalidade informática no Brasil, também está-se diante de outro tema de fraca pesquisa nacional: a vitimodogmática e, *a fortiori*, a

criminologia. O raciocínio do papel influente da vítima diante do crime, todavia, requer o estudo a partir do conhecimento prévio da teoria funcionalista, que aumenta o espectro de variáveis para o estudo do crime, permitindo que acresça-se outros aspectos sociais ao estudo que não somente a relação de causalidade e a finalidade do agente da conduta.

Diante de tal quadro, socorrer-nos-emos nas doutrinas internacionais, em especial a alemã e espanhola, para que, situando-nos dentro da ideia funcionalista, tenha-se a permissão para acrescentar o elemento “comportamento da vítima” no estudo da tipicidade penal, mais especialmente a figura da “autocolocação em risco”.

Também é na doutrina estrangeira européia, norte-americana, australiana e sul americana que se buscou socorrer, quanto ao estudo da criminalidade informática graças ao atraso legislativo pátrio e às poucas pesquisas de campo.

Para a criminologia, buscaremos a doutrina brasileira, mexicana, venezuelana, espanhola, britânica e norte-americana para apoio.

Especialmente no que se refere à vítima, apresentaremos em breves linhas a vitimologia, fazendo um corte para a vitimodogmática e demonstrando a dupla penal vítima-vitimário e suas relações nas condutas apresentadas.

O ainda conservadorismo ultrapassado dos tribunais e intelectuais que resistem em estudar e conhecer as novas doutrinas penais mais pensadas e adaptadas à realidade social leva à margem a apreciação da vítima.

O intuito será limitar o tema à explanação da criminalidade informática em seus aspectos fundamentais com a ótica informática da criminalidade comum e as particularidades para interpretação de tal modalidade criminosa, na sequência apresentando novas condutas humanas que, por conta do evoluir dos valores, passam a ter natureza de violadoras de bem jurídico e assim ganham relevância para o Direito Penal na maioria das soberanias.

A conclusão do trabalho será um apanhado geral do cenário da criminalidade em pauta, dos principais delitos informáticos já tipificados no mundo ocidental, terminando em demonstrar a necessidade de ação do Estado e da sociedade para ambos os personagens participantes da conduta que gera violação.

O trabalho que é desenvolvido a partir destas linhas visa avaliar os riscos e as responsabilidades trazidos pelo ingresso da informática na vida dos cidadãos, bem como os papéis que cada ator interpreta na situação tecnológica, demonstrando, assim, que os delitos informáticos devem ser vistos com olhos mais abrangentes do que aqueles voltados exclusivamente para a figura do autor da conduta. Diversas expressões utilizadas no decorrer da evolução das ideias são apresentadas em língua inglesa, uma vez que a doutrina as acatou e não buscou sinônimos explicativos. Para que a leitura não fique prejudicada, portanto, quando expressões restritas ao universo do Direito Informático surgirem, as definiremos em nota de rodapé e/ou, ao final, o leitor contará com um glossário de definições.

Em sua primeira parte, será apresentada muito brevemente a conceituação da eletrônica e informática na sociedade; na sequência apresentar-se-á aquelas características que considera-se fundamentais para o novo espectro informático do Direito Penal, para então classificar-se a concepção de delito eletrônico de acordo com análise dos alguns autores que se dignaram de escrever sobre o tema. Na sequência, será dada atenção aos principais tipos internalizados pelas legislações estrangeiras, comparando-os com nossa legislação na medida do possível.

Na segunda parte, a dissertação traz uma pesquisa sobre a vitimologia e a vitimodogmática, demonstrando-se, assim, sua importância, relevância, e apresentando a boa tendência científica de regressar o pensamento de considerar a vítima como relevante no estudo do crime e suas minúcias.

Em seguida, os institutos de participação da vítima são analisados sob os enfoques do consentimento do ofendido e da autocolocação da vítima em risco, e sua influência e aplicabilidade nos delitos informáticos serão apreciados, apontando-se para a necessidade de um Princípio vitimológico.

Finalmente, o estudo será concluído pela necessidade de criação e adaptação legislativa, pelas consequências jurídicas da aceitação da vitimodogmática na tipificação de delitos, para então propor mudanças de política criminal para os casos em que a vítima tenha seu comportamento relevado nas condutas, bem como formas de contenção de criminalidade, sempre cuidando por tentar trazer a criminologia para tais interpretações.

A SOCIEDADE DE RISCO INFORMÁTICA

A informática é o emprego do tratamento automático das informações¹³. Isto posto, é de se entender que o uso, a transformação e a transmissão ampla de informações, para ser difundida de maneira global e universal, exige que a forma utilizada para que tal procedimento ocorra seja também difusa e uniforme.

Para que a indústria de tecnologia informática crescesse e se difundisse, foi necessário que se chegasse a um ponto comum, qual seja, a criação e desenvolvimento de tecnologias com pressupostos e linguagens semelhantes e capazes de se intercomunicar.

Com isso, mais e mais os aparelhos tecnológicos passam a interagir e trocar informações automaticamente e entre si com o passar do tempo. E isso não se deu por acaso.

A rede mundial de computadores é posterior à computação, por certo. Foi ela o primeiro e principal passo dado pelo homem para intercomunicar aparatos, permitindo a troca de informação facilmente. Isso se deu com base na aceitação global de uma mesma linguagem adotada por todos os computadores denominada “Protocolos TCP/IP¹⁴”.

Não seria errado afirmar que em um dado momento do passado, diferentes tecnologias foram desenvolvidas em diferentes núcleos do planeta, cada qual com linguagem própria e com sua forma de codificar as informações.

Num paralelo reverso com a figura católica da Torre de Babel¹⁵, as tecnologias

¹³ Conforme dicionário Michaelis *on line* disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php?palavra=inform%E1tica>. Acesso em 03.01.09 às 01:33hs.

¹⁴ TCP/IP é sigla que significa “*Transmission Control Protocol/Internet Protocol*”, ou “protocolo de controle de transmissão/ protocolo de internet” e que nada mais é do que uma série de mecanismos desenvolvido para interconectar e compartilhar dispositivos através das redes.

¹⁵ Há uma curiosa passagem da bíblia que nos serviria de metáfora inversa, tendo-se em vista que o caminho de unificação de linguagem informática foi uma realidade. Em dada passagem, o SENHOR, nota que os seres humanos falavam a mesma língua e, portanto, não havia nenhum tipo de restrição para aquilo que quisessem fazer. O homem almejavam construir uma torre para tocar o céu e, por falarem a mesma linguagem, iniciam a obra e a desenvolvem com sucesso. O SENHOR, então, faz com que as pessoas passem a falar línguas diferentes para que, assim, não consigam atingir seu ideal. E assim é: “*E era toda a terra de uma mesma língua e de uma mesma fala./ E aconteceu que, partindo eles do oriente, acharam um vale na terra de Sinar; e habitaram ali./ E disseram uns aos outros: Eia, façamos tijolos e queimemo-los bem. E foi-lhes o tijolo por pedra, e o betume por*

inicialmente eram montadas em linguagens diferentes, e eram incapazes de trocar informações, relacionarem-se e compreenderem-se automaticamente.

O advento da uniformização da linguagem informática, então, surge para resolver o problema e permitir que aparatos e redes de aparatos interliguem-se entre si e, pois formem um conjunto harmônico de mecanismos de trocas de informações.

Inicialmente, a interligação em escala larga se deu em 1969, nos Estados Unidos, com o desenvolvimento militar da ARPANET – *Advance Research Projects Agency Network* ou Rede da Agência de Pesquisa de Projetos Avançados –, uma experiência no auge da Guerra Fria que permitiria que pesquisadores de diversos centros de pesquisa pudessem compartilhar recursos, sem risco de ter os dados e informações perdidas por conta de um eventual bombardeamento inimigo em um centro¹⁶. Assim, a ideia foi a de difundir a informação sem que houvesse somente um único centro estratégico frágil que, atacado, levaria a um caos desenvolvimentista, permitindo-se que a informação trafegasse mesmo que tivesse havido a perda de um ou alguns núcleos tecnológicos. Pode-se dizer, portanto, que a importância inicial da rede informática foi estratégica.

No início da década de 1980 houve uma separação da rede, dividindo-se em ARPANET e Milnet, sendo a segunda uma rede dedicada exclusivamente à troca militar de dados; em 1986, os supercomputadores da NSF – *National Science Foundation* ou Fundação Nacional de Ciência – foram interligados com os da ARPANET¹⁷ criando-se a espinha dorsal (*backbone*) da rede formada por um feixe de computadores superpotentes, permitindo-se a

cal./ E disseram: Eia, edifiquemos nós uma cidade e uma torre cujo cume toque nos céus, e façamo-nos um nome, para que não sejamos espalhados sobre a face de toda a terra. / Então desceu o SENHOR para ver a cidade e a torre que os filhos dos homens edificavam; / E o SENHOR disse: Eis que o povo é um, e todos têm uma mesma língua; e isto é o que começam a fazer; e agora, não haverá restrição para tudo o que eles intentarem fazer. / Eia, desçamos e confundamos ali a sua língua, para que não entenda um a língua do outro. / Assim o SENHOR os espalhou dali sobre a face de toda a terra; e cessaram de edificar a cidade. / Por isso se chamou o seu nome Babel, porquanto ali confundiu o SENHOR a língua de toda a terra, e dali os espalhou o SENHOR sobre a face de toda a terra”. (Gênesis 10:1)

¹⁶ CASTELLS, Manuel. A Sociedade em Rede. Volume I. Paz e Terra, 1999, pp. 82-83.

¹⁷ Em 28 de fevereiro de 1980, os computadores da ARPANET são desconectados do sistema, tornando a INTERNET uma rede totalmente privatizada, sem controles militares ou governamentais. Com isso, algumas entidades como, por exemplo a ICANN - *Internet Corporation for Assigned Names and Numbers* – passaram a assumir, não oficialmente, a regulamentação do ciberespaço, ao menos quanto à padronização e alguns regramentos.

expansão da rede como se conhece, no final da década de 1980¹⁸.

A rede iniciou-se como canal de trocas de informações notadamente escritas, além de arquivos e programas. Sequencialmente, em 1989, Tim Berners-Lee, um cientista inglês que trabalhava na *European Organization for Nuclear Research* (Organização Européia para Pesquisa Nuclear) na Suíça, desenvolveu um complexo sistema de documentos interligados que misturava texto, imagem, som e mídia e se inter-relacionava através da Internet, por meio de ligações (*links*) que poderiam ser acionadas, levando o usuário conectado à Internet a trafegar por diversos ambientes e plataformas diferentes, num ambiente visual, mais rico e amigável. Essa tecnologia foi lançada em 1992 e conquistou os usuários por sua versatilidade, recebendo o nome de *world wide web* (larga teia mundial) ou simplesmente *web* e popularmente conhecida pelas letras “www”.

Desta forma, é possível que se entenda a Internet como sendo um suporte, uma superautopista¹⁹ caracterizada por três elementos: a) ser uma cadeia de redes interligadas entre si, b) existir em escala mundial e c) em que os equipamentos se comunicam através de uma mesma linguagem permitindo-se a circulação de informações através conversões sequenciais.

A popularização foi tamanha, que a nova ferramenta fez com que em três anos a Internet atingisse a marca de 50 milhões de usuários, cifra que somente foi atingida pelo rádio após 37 anos e pela televisão, em 15²⁰.

Os motivos são muitos.

Um bom motivo é o fato de que a Internet é uma sociedade ideal em tese. Todos seriam iguais e anônimos. Todos teriam as mesmas condições num meio em que condição social e aparência são irrelevantes. Todos seriam concomitantemente alguém e ninguém na rede.

Entretanto, diferentemente da sociedade material em que posse, sorte, influência e

¹⁸ CASTRO, Carla Rodrigues Araújo. Crimes de Informática e seus Aspectos Processuais. 2ª Edição. Ed. Lumen Juris, Rio de Janeiro, 2003, pp. 2-3.

¹⁹ Apelidada pelos norte-americanos de “*Superhighway*”.

²⁰ “As John Naughton (1999) points out, it took the World Wide Web just three years to reach its first 50 million users; a feat which eluded television for 15 years and which took radio 37 years to achieve from its point of inception”. JEWKES, Yvonne. Policing the Net: crime, regulation and surveillance in cyberspace. In Dot.cons. Willan Publishing, Devon, 2002, p. 33.

chance ditam as oligarquias de um poder pré-constituído e onde somos obrigados a assinar um contrato social, na sociedade virtual as regras iniciais e as limitações são mínimas ou até mesmo inexistentes.

Respeitadas as devidas proporções²¹, não há abdicação de parte da liberdade virtual do usuário em prol de uma autoridade centralizadora que comanda e rege, impõe limites, pune e barra atitudes²². Ao contrário, a rede traz a possibilidade de identidade multidimensional e amorfa, podendo cada um ser quem quiser, o que quiser e quando quiser, permitindo que cada um seja autor de sua própria personalidade virtual²³.

Enquanto que no mundo real há que se passar por uma porta giratória com detector de metais para se ingressar em um banco, o ingresso em qualquer instituição da sociedade virtual – seja financeira, seja governamental ou outra – está a um clique de distância.

Inimaginável para a maioria considerar entrar em ambientes nobres na vida humana material. Para muitos, na vida real, é impraticável viajar para o exterior e ver novas culturas e paisagens. Tais práticas sempre foram consideradas para poucos, geralmente abastados e, assim, para uma classe social pequena, dominante e controladora.

Mas a rede mundial levou a todos os usuários a noção ideal do Princípio da Igualdade: enquanto que a doutrina expõe tal Princípio como aquele que pugna tratar iguais igualmente e desiguais desigualmente, na informática a segunda parte do brocardo não existe: não existem desiguais na anonimidade virtual. Todos podem acessar *sites* de turismo, visualizar fotos de monumentos, quadros, paisagens e até mesmo ingressar virtualmente no gabinete de uma presidência de república. Tanto um milionário quanto um assalariado acessam o mesmo *site*, vêem as mesmas coisas e buscam informações com a mesma possibilidade e na mesma condição.

²¹ A Internet existe inserta em um mundo tangível e, portanto, acaba se submetendo às tais regras pré-existentes, mas em proporção inferior por conta do exíguo controle e fiscalização.

²² Vale citar, aqui, opinião diversa de Michael McConnell, Diretor Nacional de Inteligência dos Estados Unidos da América que em artigo de 21 de janeiro de 2008 manifestou-se no sentido de defender que a Internet seja totalmente controlada pelos Governos. Acesso em http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright em 07.04.2008 às 17:36hs.

²³ JEWKES, Yvonne e SHARP, Keith. Crime, deviance and disembodied self: transcending the danger of corporeality. In Dot.Cons. Willan Publishing, 2002, Devon, p.2.

Certamente que há segmentos “*on demand*²⁴”, exclusivos e que têm custos ou assinaturas. Mas diferentemente de na vida real, qualquer sociedade restrita é acessível a um usuário com algum crédito. O proprietário de um carro esporte de luxo não é ninguém diferente numa sala de bate papo. O pobre pode fingir-se rico, o culto pode fingir-se ignorante. E o fingimento é irrelevante em um universo em que todos são idealmente representados por uma sequência de números denominada *Internet Protocol* (IP).

A uniformidade e a homogeneidade da rede tornam todos humanos idênticos: as limitações da deficiência física, da cor, da religião, da idade, da estética e da condição social são irrelevantes no mundo virtual.

Todos têm os mesmos direitos e podem alçar-se e destacar-se por méritos e habilidades, sem berço esplêndido. E todos se misturariam num mesmo meio, sem preconceito aparente.

Porém, a imagem apresentada nas linhas acima tem uma lacuna: apesar de potencialmente a rede ser uma meritocracia de idênticos, a informação e o conhecimento da linguagem adotada pela rede dão poder ao usuário antes comum.

Uma pessoa de grande importância na sociedade material, se for ignorante quanto às minúcias da manipulação de dados e da programação, na Internet é apenas um usuário comum; enquanto que um comum do povo, com conhecimento, pode pertencer a uma elite cibernética.

Mínimo é o número de usuários que explora todos os recursos de suas máquinas. Não raro o usuário nunca leu o manual de instruções de seu aparelho de telefonia celular. O usuário de computadores apressa-se em somente conhecer o mínimo para se comunicar, navegar por páginas de reduzido interesse e quiçá utilizar-se de recursos multimídia, descartando a potencialidade de seu aparelho informático.

É da natureza humana o conceito de *satisfying* trazido modernamente pela teoria das escolhas da economia²⁵. A racionalidade humana, em sua maioria, satisfaz-se com o mínimo

²⁴ Tradução livre: “sob demanda” ou “a pedido”.

²⁵ Desenvolvida por Herbert Alexander Simon, prêmio Nobel de economia em 1978, trata do processo de tomada

suficiente para que consiga seus objetivos, sem importar-se com atingir o ponto máximo do conhecimento ou compreender todo o ambiente que o cerca.

Destarte, raros são os usuarios de máquinas que aprofundam e compreendem amplamente as potencialidades de seus petrechos²⁶. O mesmo ocorre na rede mundial de computadores que é modulada por linguagens e padrões de assimilação e processamento de dados. Poucos se esforçam para conhecer a Internet largamente e, aqueles que o fazem, passam a ter a pedra fundamental para disponibilidade e manipulação da vida virtual, passando a ter certo controle neste segmento da sociedade.

Um programador de classe baixa ou um intelectual não engajado, em regra não almejam ingressar na carreira política para comandar o Poder Executivo ou Legislativo por ser uma pretensão provavelmente inatingível. Não é a intelectualidade necessariamente que leva alguém aos degraus mais altos do poder. Na rede, entretanto, o conhecimento específico de tais sujeitos pode fazer a diferença. O poder virtual²⁷ é pessoal e depende da capacidade individual de manipulação de dados e compreensão de linguagens: o meio é objetivo.

Certamente há diversos núcleos sociais, cada qual com seu conteúdo ético. Cada indivíduo participa de círculos de convívio por simpatia, cada qual com suas regras particulares. Muitos dos círculos sociais se interpenetram, uma vez que cada indivíduo participa de diversos (clube, time de futebol, profissão, amizades, etc).

A Internet, porém, é universal e inevitável. É um grande círculo que abarca todos os outros círculos sociais que queiram e aceitem utilizá-la para melhor comunicação entre pares e é, também, um círculo de participação obrigatória para aqueles que seguem a evolução

de decisão a partir do raciocínio de que os indivíduos, ao invés de fazerem escolhas a partir da ideia de maximização de bem estar, buscam decisões focadas em objetivos “suficientemente bons” (satisfying) para si. MONTEIRO, Jorge Vianna, artigo disponível em <http://ppe.ipea.gov.br/index.php/ppe/article/viewFile/545/489>. Acesso em 02.01.09 às 01:47hs.

²⁶ Aqui vale citar Ian Murphy, considerado um dos primeiros *hackers* da história, que em 1981 invadiu o sistema da empresa AT&T e modificou seu horário oficial, atrasando 12 horas e, pois, levando a que todos os telefonemas feitos no horário de pico fossem cobrados com tarifas mais baixas, correspondentes a horários tardios em que se costuma elaborar políticas de incentivo ao uso. A mudança foi descoberta alguns dias depois, mas a empresa registrou prejuízo de milhões de dólares. Fonte: <http://www.wired.com/science/discoveries/news/2001/02/41630> Acesso em 16.04.08 às 12:11hs.

²⁷ Por poder, aqui, referimo-nos, dentre tantas outras habilidades, à capacidade de sobrepujar outros usuarios, controlar máquinas, derrubar ou paralisar sites, criar notícias, acessar sites restritos, modificar integridade e, assim, ganhar fama e reconhecimento no meio.

cultural da humanidade. Dentro da própria rede há também sub-círculos de interesse, por vezes até mesmo organizados nas denominadas redes sociais²⁸.

A sociedade informática está inserida no contexto social material (físico), e tem seus limites de conduta traçados pela legislação vigente. Assim como numa família há regras ditadas pelos próprios familiares em sua micro-célula, a Internet e as redes de comunicação informática também possuem suas formas de conduta e porte.

Hodiernamente não há um normativo trans-soberano que demonstre regras de comportamento na rede informática. Apostou-se por muito tempo que as redes e seus participantes seriam capazes de se auto-regular, simplesmente por seu agir comunicativo, mas a realidade não se mostrou tão simpática.

O poder (da informação) dado ao conhecedor da linguagem e procedimentos fez com que se experimentassem abusos na rede, ultrapassando os limites razoáveis do bom convívio, numa repetição das ideias de Maquiavel²⁹. A importância que as informações transformadas em *bits* tomou, dada a imprescindibilidade da rede, fez com que dados passassem a ter alto valor econômico; e conforme o meio virtual toma força e substitui as esferas da vida material, mais e novos dados são incluídos e cobiçados. A rede então passa a ser alvo da cultura delinquente.

Há que se admitir que houve algum esforço para regramento da nova sociedade: um único normativo apresentado e adotado de modo costumeiro na sociedade da informação foi o documento particular denominado “*Netiquette Guidelines*”³⁰, elaborado por Sally Hambridge e aceito como principal concentrador de regras de conduta nesse meio ambiente³¹.

²⁸ São exemplos o MySpace, o Orkut, o Flickr, o Facebook, o Friendster, etc. Uma lista ampla pode ser encontrada em http://pt.wikipedia.org/wiki/Lista_de_redes_sociais. Acesso em 08.06.08 às 19:47hs.

²⁹ MAQUIAVEL, Nicolau. O Príncipe. Editora Martins Fontes, 2ª Edição, São Paulo, 2001, *passim*.

³⁰ Ou Normas de Netiqueta, produzidas nos Estados Unidos da América (Califórnia) está disponível originalmente em <http://asg.andrew.cmu.edu/rfc/rfc1855.html>. Acesso em 01.02.08 às 02:36hs, com tradução para português em <http://www.g2ctech.com/artigos/RFC1855.html>. Acesso em 01.02.08 às 02:37hs.

³¹ Marco Antonio Zanellato, em seu artigo Condutas Ilícitas na Sociedade Digital, aponta que em 2002 poder-se-ia contar com uma norma de Princípios éticos denominada NRPOL – Norma de Referência da Privacidade Online, desenvolvida em junho de 2000 pela Fundação Carlos Alberto Vanzolini, ligada à Escola Politécnica da USP, que trazia os seguintes Princípios no tocante às informações particulares dos usuários: “a) as informações pessoais identificáveis podem ser obtidas para um ou mais propósitos e devem ser coletadas por meios éticos e legais, b) o propósito da coleta de informações pessoais identificáveis deve ser especificado antes do instante desta coleta, c) as informações pessoais identificáveis solicitadas devem ser adequadas, relevantes e não superar

As regras contidas no normativo referido são importantes para uma conduta respeitadora do meio ambiente informático. Contudo, estão bastante desatualizadas no que diz respeito às novas tecnologias. De qualquer modo é nesse normativo informal que se encontram sugestões de normas de comportamento moral virtual, certamente de maneira não cogente.

O principal mérito da proposta da “*Netiquette Guidelines*” é o de demonstrar claramente o fato de que a Internet (e há que se assumir que todo o meio de comunicação informático), apesar de virtual, é deveras similar ao mundo físico e exige os cuidados naturais de convívio e preservação.

Na leitura, a comunicação na rede é lembrada com a característica de ser feita entre seres humanos³² e que se deve fazê-la de maneira especial, mas com grande semelhança com a vida material: lembra, por exemplo, que ao responder uma mensagem coletiva, deve-se ler com cuidado o remetente para que não se viole a intimidade alheia, expondo alguém e ferindo-lhe a honra; aponta o fato de que há que se respeitar a extensão das mensagens enviadas para não onerar excessivamente o destinatário e assim por diante.

Apesar de o normativo não ser oficial, ele apresenta com muita razão o fato de que a sensação de distância e segurança trazida pela eletrônica não implica um descuido quanto à postura (ao menos de etiqueta) social a ser adotada.

E o fato de se fazer referência à rede mundial de computadores como uma mera extensão da sociedade, estende-se, naturalmente, pensamentos como o de que *mutatis mutandi*, a Internet é consequentemente uma sociedade de risco “*sui generis*”.

os objetivos para os quais são coletadas, d) as informações pessoais identificáveis coletadas devem ser mantidas íntegras, conforme fornecidas pelo usuário, e) as informações pessoais identificáveis devem ser atualizadas quando necessário ou quando for solicitada pelo usuário, f) a Organização deve ter uma política explícita de práticas e procedimentos com relação aos dados pessoais identificáveis de seus usuários, g) a Organização deve tomar medidas técnicas e organizacionais para evitar a utilização desautorizada ou em desacordo com a lei e contra a perda accidental, destruição ou dano das informações pessoais identificáveis de seus usuários, h) devem ser observados rígidos limites éticos na divulgação e utilização de informações pessoais sensíveis dos usuários, i) o usuário deve ter acesso às informações pessoais identificáveis por ele fornecidas, e j) o usuário deve ter mecanismos para comunicar-se com a Organização que coletou seus dados pessoais identificáveis.” In Direito & Internet. Escola Superior do Ministério Públicos de São Paulo, São Paulo, 2002, pp. 217-218.

³² Cabe elucidarmos que, em verdade, a comunicação é feita entre endereços de IP e, portanto, entre locais em que se situam geograficamente máquinas. Dizermos que a comunicação é feita entre seres humanos não significa necessariamente que ambos estejam presentes no momento do envio de mensagem, arquivos, etc, mas sim que tal relação – seja entre presentes, seja entre ausentes – intenta relacionar pessoas, cada qual guarnecida por um aparelho com a função de facilitar e agilizar tal contato.

A denominação “sociedade de risco” foi tecida inicialmente por Ulrich Beck³³ que, ao abordar a evolução industrial frente ao acidente com gases letais ocorrido em uma cidade da Índia em 1984³⁴, trouxe a ideia de que há uma verdadeira e necessária troca (*trade-off*) por conta da evolução social.

Desta maneira, o autor defende que para uma sociedade evoluir e haver continuidade na produção de riqueza, faz-se necessário o avanço tecnológico e a exploração de novas áreas. A crescente industrialização traz consigo, então, escolhas, e estas são relacionadas às consequências e, logo, a sacrifícios. De acordo com tais ideias, para que haja pneus, é necessário poluição; para que haja tráfego viário, é necessário que haja trânsito e perigos e assim por diante.

Ocorre que a teoria avança. A identificação de custos sociais decorrentes do desenvolvimento já fora identificada pela economia. Contudo, apresenta Beck que a nova sociedade tem consciência de que vive em constantes riscos e é capaz de identificá-los, e sucessivamente lidar com tais riscos, elaborando normas que buscam mitigar os custos consequentes das modernidades³⁵.

O desenvolvimento levou o ser humano a elaborar tecnologias, e simultaneamente ser capaz de detectar os riscos advindos de tais avanços, etiologicamente, tornando-nos capazes de assumir posturas de evitação de riscos desnecessários e de contenção de atitudes capazes de elevar a quantidade mínima de riscos aceitáveis para o evoluir social³⁶.

Consegue o ser humano identificar causas e efeitos decorrentes de relações sociais como exemplificativamente o uso de motores a combustão e buscar normativos

³³ BECK, Ulrich. *La Sociedad Del Riesgo*. Tradução Jorge Navarro *et al.* Editorial Paidós, Barcelona, 1998, 25-26 (publicado originalmente por Suhrkamp, Francfort Del Meno, Bonn, 1986).

³⁴ Na noite entre dois e três de dezembro de 1984, cerca de 40 toneladas de metil isocianato e outros gases letais vazaram da fábrica de agrotóxicos da Union Carbide Corporation, em Bhopal, Índia. Foi o pior desastre químico da história. Estima-se que entre 3,5 e 7,5 mil pessoas morreram em decorrência da exposição direta aos gases, mas o número exato continua incerto. Infelizmente, a noite do desastre foi apenas o início de uma tragédia, cujos efeitos se estendem até hoje. A Union Carbide, que possuía a fábrica de agrotóxicos na época do vazamento dos gases, abandonou a área, deixando para trás uma grande quantidade de venenos perigosos. Os moradores de Bhopal ficaram com fornecimento de água contaminada e um legado tóxico que ainda hoje causa prejuízos. Fonte: Greenpeace http://www.greenpeace.org.br/toxicos/pdf/bhopal_desastrecont.pdf. Acesso em 13.04.08 às 19:33hs.

³⁵ BECK, Ulrich. Op. cit. p. 26.

³⁶ BECK, Ulrich. Op. cit. pp. 26, 29-31.

transoberânicos como o protocolo de Kyoto assinado em 1997, levando às administrações (públicas e privadas) maior tato na tomada das decisões, vez que previsão de riscos passa a ser raciocínio natural e obrigatório, por vezes levando a custos e responsabilizações por omissão na identificação ou danos advindos³⁷.

A ideia de sociedade de risco adéqua-se perfeitamente ao segmento virtual de convívio criado pelo advento da interligação de equipamentos eletrônicos formando a rede mundial de computadores, a Internet. O uso da nova tecnologia representa risco como qualquer outra conduta³⁸.

A sociedade da informação teve sua potência elevada com a popularização das máquinas e suas conexões, levando à boa parte da população o acesso a um cotidiano com características próprias, e que tem arquivos intangíveis como mote de sua existência e sustentabilidade. A rede mundial de computadores trouxe velocidade de relacionamentos (comerciais, negociais, humanos, internacionais, etc) e dissolveu fronteiras físicas, permitindo que o usuário-internauta experimentasse liberdade em grau antes inimaginado.

O acesso às informações, vídeos, fotos, filmes, a potencialização da possibilidade de comunicação e a sensação de segurança fizeram com que houvesse massiva popularização da rede. Certamente, todavia, a evolução tecnológica trouxe consigo sacrifícios e riscos.

Entusiasmada com a nova ferramenta³⁹, a sociedade aderiu às novas práticas ofertadas pela informática, adquirindo rapidamente computadores e celulares, absorvendo com gigantesca demanda a tecnologia⁴⁰. Nota-se, contudo, que a compreensão dos riscos da sociedade, em se tratando de sociedade da informação, ainda não foi bem compreendida.

³⁷ Aqui cabe citar exemplificativamente a tendência mundial de responsabilização de indústrias tabagistas pela morte dos fumantes, afastando-se ser a contribuição do ofendido imprescindível para a descaracterização da obrigação de indenizar por parte das empresas. Exemplificativamente, temos a Apelação Cível TJRS nº 70016845349, relatora Des.^a Marilene Bonzanini Bernardi.12.12.2007,

³⁸ Conforme LUHMAN, Soziologie des Risikos, Berlin, 1991, *passim*. Apud QUIROGA, Jacobo López Barja de. El moderno derecho penal para una sociedad de riesgos. *Poder Judicial*, n. 48, s.l., 1997, p.221.

³⁹ O pesquisador e demógrafo canadense Don Tapscott pesquisou o comportamento das pessoas frente à tecnologia e as classificou em 4 gerações (*baby boomers*, geração X, geração Y e geração Z). As gerações Y e Z, especialmente, são aquelas que viveram imersas na eletrônica e no conteúdo digital, respectivamente, mostrando-se dependente da informática em seu cotidiano. Fonte: Revista INFO, dezembro de 2008, pp. 50-55

⁴⁰ Segundo estudo do IBOBE/NetRatings, o número de internautas residenciais ativos em fevereiro de 2008 cresceu 4,5%, atingindo 22 milhões de usuários, 56,7% mais do que em fevereiro de 2007. <http://www.ibope.com.br/calandraWeb/servlet/CalandraRedirect?temp=6&proj=PortalIBOPE&pub=T&nome=h>

Há de se considerar que muitos dos riscos da sociedade virtual são intangíveis como o próprio meio e desta forma têm sido mais dificilmente percebidos pelos cidadãos virtuais. A contrário senso, a indústria exploradora da tecnologia informática utiliza-se da estratégia de venda para mitigar os riscos dessa sociedade “*sui generis*”, reforçando ao usuário a sensação de proteção e de segurança além daquela inerente à relação impessoal e anônima, mascarada pela tela do computador⁴¹.

Ao se tratar da segurança do meio informático, cabe fazer algumas reflexões de fundamental importância para se compreender o risco da Internet.

Em primeiro lugar, deve-se defender a existência de fundamental diferença entre a sensação de segurança e a segurança como realidade. Para compreender-se, é importante citar-se que tais figuras não necessariamente co-existem. Pode-se sentir seguro sem na realidade estar seguro e pode-se estar seguro e na realidade não se sentir.

O antivírus e o *firewall* ligados ou ativos por vezes passam a percepção de proteção, mas ao rodar um programa com falha de segurança, fica o sistema vulnerável a ataques além da capacidade dos protetores. Há sensação de segurança sem que esta exista. Da mesma maneira, o ingresso e permanência em um *site* pode passar a impressão de que se está sob risco, quando na realidade não se está.

O escudo que a tela do computador representa, não raro traz ao usuário a sensação de segurança, dando aparência de inatingibilidade. Não estar exposto em suas fragilidades faz com que prevaleça a ideia de segurança e o ser humano tenda a agir com menos limites e maior ousadia em tal situação. A economia justifica tal conduta com a figura da “*moral hazard*”, ou risco moral.

[ome_materia&db=cald&docid=2CBC3F5579CD61888325742700479B37](#) Acesso em 14.04.08 às 01:55hs.

⁴¹ Cabe aqui citarmos o escândalo que veio à tona quando da denúncia feita contra a empresa Sony que, em 2005, vendeu um CD de músicas que continha um *rootkit* que se instalava veladamente no computador do usuário para impedir a cópia ou compartilhamento das trilhas adquiridas numa tentativa de evitar a violação de direitos autorais. A empresa, contudo, ao inserir o *rootkit* abriu brechas de segurança no sistema operacional Windows e o fez de forma que os sistemas antivírus não conseguissem detectar tal código malicioso. Há também, no sentido oposto, a ideia de crime como mercado. A impingência de medos na população através de propagandas, gera conceitos de uma verdadeira indústria de vitimização que faz com que o mercado de segurança tenha seu desenvolvimento econômico alavancado. WALKLATE, Sandra. Perspectives on the Victim and Victimisation. In Handbook of Victims and Victimology. Willan Publishing, London, 2007, pp. 14-15.

Por tal expressão entende-se a figura que reporta o fato de que o ser humano tem comportamentos mais arriscados e mais ousados motivados por um excesso de confiança que é trazido ao indivíduo por conta de uma sensação. Empiricamente, pode-se dizer que a sensação de tranquilidade (ou aparência de tranquilidade) quanto a uma situação faz com que indivíduos ajam com menor cautela e responsabilidade⁴².

Tal figura se mostra atual especialmente na forma como conduz o internauta sua navegação. Quando se sente protegido ou não sente que tem algo a perder, o usuário médio porta-se com menor cuidado, navegando em sítios despreocupadamente, perdendo cautelas para abrir *emails* de desconhecidos, para clicar em anexos entre outras tantas atitudes.

Um paralelo com a criminalidade dita comum. Não raro a figura do delinquente é representada por alguém que se esconde. O uso de máscaras por foras-da-lei, o uso da meia de seda na cabeça para o gatuno, o encapuzamento do sequestrado, todas são condutas que intentam evitar que as características identificadoras dos infratores fiquem à vista. Sente-se mais seguro e com menos amarras o sujeito que se esconde, portando-se assim sem os limites normalmente impostos⁴³.

Importante notar que a rede mundial de computadores dá a todos o véu da anonimidade. E a sensação de esconderijo traz ínsita a ideia de oportunidade de agir sem ser percebido, numa sensação de segurança. É, todavia, realidade dúplice, porque dá ao delinquente a sensação de anonimidade pretendida, ao mesmo tempo em que dá à vítima a sensação de segurança porque não visualiza claramente os riscos.

⁴² O principal exemplo trazido pela ciência econômica é o do seguro: um indivíduo que tenha seguro contra incêndio sente-se mais propenso a tomar menos cautelas quanto à sua residência e o uso de materiais inflamáveis, chegando-se até ao extremo de alguém que atea fogo em sua própria residência para receber o prêmio do seguro. Também é exemplo o fato de que pessoas que possuem seguro de automóvel tendem a tomar menos cuidado quanto aos locais escolhidos para estacionamento. PINDYCK, Robert S. e RUBINFELD, Daniel L. Microeconomia, 5ª Edição, tradução Eleutério Prado, Prentice Hall, São Paulo, 2002, pp. 613-615; também VARIAN, Hal R. Microeconomia – Princípios Básicos, tradução da 6ª Edição, 5ª tiragem, Editora Campus, São Paulo, pp. 722-725.

No mesmo sentido, pesquisa espanhola demonstra que o índice de comunicação e registro de roubos e furtos cometidos contra pessoas que possuem apólices de seguro é significativamente inferior a daquelas que não possuem. STRANGELAND, Per. *Criminología realista y El problema de las víctimas*. In Problemas criminológicos em las sociedades complejas. Universidad Publica de Navarra,*- Espanha, 2000, p. 142.

⁴³ Certamente em muitos casos é o uso de substâncias entorpecentes que dá ao sujeito a sensação de quebra de limites, também. Nesse sentido, a ideia da agravante da embriaguez pré-ordenada do artigo 61, “i” do Código Penal. Contudo, compreendemos que o uso de tais substâncias serve também para mascarar (ou esconder) a personalidade respeitadora de limites, forçando condutas mais liberais.

Some-se a estes fatos a dificuldade de o usuário compreender o valor das informações produzidas nos meios telemáticos, e tem-se a combinação perfeita para uma conduta delitiva⁴⁴.

É interessante notar que ao andar-se na rua, o surgimento de um sentimento de desconfiança no ambiente ou em alguma pessoa a vista, leva à fuga ou a busca por abrigo. O senso de perigo e a análise das pessoas e da situação ao redor permitem que, por vezes, identifique-se o problema e o evite. Isso ocorre porquanto o ser humano está familiarizado e conhece o meio físico, sendo capaz de entender os acontecimentos e riscos. O criminoso, ainda que instintivamente, conhece essa realidade e vale-se do elemento surpresa para que sua conduta não permita reação da vítima.

Trazendo o mesmo raciocínio para o Direito Penal Informático notadamente ver-se-á que isso não se aplica. O usuário vítima não sabe onde está na rede porque não está em lugar algum e ao mesmo tempo em todos. Endereço fixo somente há do ponto de partida de cada usuário (IP), ou seja, em uma máquina que adquire permissão para acessar a rede através de um provedor.

O mesmo ocorre para o criminoso, com o diferencial de que para o agressor há o interesse em estar oculto e há vezes em que, na rede, seu conhecimento em manipular as informações dificulta ainda mais sua localização ou elimina as provas do fato.

Destarte, a grande maioria dos internautas vaga por endereços virtuais sem ser capaz de ponderar o quão seguro está e o quanto é prudente permanecer se embrenhando em tais

⁴⁴ A informação, transformou-se numa grande commodity, levando a criação de certos sites com o intuito exclusivo de alienação de informação pessoal. Nos Estados Unidos da América do Norte há comerciantes que por uma pequena taxa estão dispostos a comerciar dados médicos, detalhes bancários, classificação de credores, antecedência criminal, documentos de veículos e licenças para dirigir, ou seja, dados de alta relevância para a escolha de vítimas. Todas essas são informações pessoais identificáveis. FINCH, Emily. *In* Dot.Cons. Willan Publishing. 2002. pp. 94-95.

Informações sensíveis ou Informações Pessoais Identificáveis são “dados de contato (nome completo, endereços, fones, emails, etc), dados de cobrança ou financeiros (numero de cartão de crédito, nível de renda, patrimônio, etc), documentos de identidade e profissionais (CPF, RG, etc), informações sócio-demográficas (sexo, idade, estado civil, dados étnicos, etc), dados médicos (históricos ou de condições de saúde, outros), escolaridade (graus e outros), imagens da pessoa e outras informações pessoais identificáveis como hobbies, áreas de interesse social, entretenimento, troca de informações (*chat-rooms*), lista de discussão, boletins, etc. São ainda consideradas informações pessoais as coletadas através de cookies e arquivso de log, quando contratadas de forma a permitir a identificação de usuário” ZANELATO, Marco Antonio. *Condutas Ilícitas na Sociedade Digital. In* Direito e Internet. Escola Superior do Ministério Público de São Paulo. 2002. p. 218

sítios. Também, quando abordado por *email*, mensagem de rede social ou até mesmo por SMS, vê no interlocutor mal intencionado a aparência neutra, quiçá a mesma de seus contatos, conhecidos, amigos, etc.

O que se quer chamar a atenção, nesta sociedade de risco, é com o fato de que se por um lado a tecnologia dá aos usuarios ampla liberdade e máxima igualdade individual, por outro lado ela retira a habilidade de se distinguir as pessoas com as quais relaciona-se virtualmente além de restringir a capacidade de diferenciar-se a sensação de segurança e a ideia de segurança como realidade.

Acrescente-se a tal raciocínio a ideia de que a rede é por si só um local que deixa a vítima vulnerável e é elemento integrante da conduta delincente. Porém, a Internet é um ambiente em que a vítima anseia por voltar seja por necessidade, seja por interesse tendo-se em vista que o abandono de tal ferramenta de integração social simplesmente não é possível⁴⁵.

Um dos principais lados considerados positivos é o de se poder frequentar quaisquer sítios sem nenhum remorso ou culpa, uma vez que não haverá conhecimento, reprimenda ou julgamento do usuario. E todos os usuarios são idênticos e meramente pelo acesso têm garantido o direito de assistir às mídias, escrever quaisquer textos, publicar quaisquer opiniões, produzir, ter contas de *email*, jogar jogos, dentre uma infinidade de possibilidades.

Veja-se, porém, que o mesmo lado positivo, a partir de um ponto de vista enviesado ao *dolus malus*, passa a ser um problema: o usuario delituoso tem acesso livre a quaisquer locais, inclusive nos computadores desprotegidos, sem qualquer impedimento ou dificuldade. Por ser um idêntico, não pode ser identificado, ficando totalmente anônimo. Fica a vítima, assim, sob ataque sem saber como impedi-lo e sem conseguir imaginar quem a viola, numa antinômica escuridão.

Curioso é notar que tanto os aspectos positivos quanto os aspectos negativos da tecnologia beneficiam a conduta delitiva. Ampla liberdade faz com que o pretenso delincente transite⁴⁶ livremente, sem qualquer restrição, por ambientes que melhor lhe aproveem.

⁴⁵ COX II, Raymond W., et al. Routine Activity Theory and Internet Crime. In Crimes of the Internet. Pearson Prentice Hall. 2008. p. 311.

⁴⁶ Nesta etapa utilizamos o verbo transitar, mas doravante buscaremos a alternativa do verbo navegar por conta de

Igualdade em grau máximo faz com que não seja possível detectar – ao menos inicialmente – qualquer vestígio que impeça um pronto envolvimento, fazendo com que a percepção do delito não seja imediata, gerando grandes dificuldades periciais de uma detecção tardia. O delinquente sente-se mais seguro agindo dentro da rede do que na realidade física, pois que corre riscos bastante menores.

Mas o mero sentir não basta. O crime exige, também, cumprimento da fase interna que se divide em 3 (três) etapas: cogitação, ponderação e resolução⁴⁷.

O delinquente que vê um sistema judiciário moroso e uma polícia pouco preparada e equipada, tende a ponderar ainda com maior tendência e de maneira favorável o cometimento do crime, levando em consideração a segurança que sente para cometer o fato: age com maior ousadia e subvaloriza os riscos, jogando com a boa probabilidade de não ser descoberto. Este é um raciocínio criminológico positivo que é feito consciente ou inconscientemente pelo agente.

O ambiente de risco notadamente representado na rede mundial de computadores, permite o mesmo raciocínio ao delinquente virtual. Contudo, conhecendo a fragilidade na compreensão social do meio virtual por parte da população, soma-se à ponderação da vantagem no cometimento do crime o fato de que o comportamento errado dos internautas facilita ainda mais as práticas delinquentes.

De um lado da relação criminosa, a ponta do delinquente avalia riscos, mormente pessoais, com o fito de verificar a probabilidade de sua empreitada criminosa trazer-lhe vantagens, sem levar-lhe a uma privação de sua liberdade.

Do outro, à vítima competiria compreender a sociedade de risco em que estão inseridos vitimários – ponderadores de riscos pessoais –, aceitando que a postura e conduta nesta realidade devem ser muito mais cautelosas e conscientes. Os riscos avaliados, neste caso,

o primeiro parecer etimologicamente mais adequado para condutas da vida material ou ideológica. O dicionário eletrônico Michaelis apresenta o verbo transitar como sendo “**1** Andar, fazer caminho, passar, viajar: *Habituei-me a transitar por aqui.* vtd **2** Percorrer: *Apenas carros militares transitam as ruas.* vti **3** Mudar de lugar, estado ou condição: *Certos políticos transitam facilmente de um para outro partido. Transitar em julgado:* o mesmo que *passar em julgado.*” <http://michaelis.uol.com.br/moderno/portugues/index.php?palavra=transitar>. Acesso em 18.06.08 às 16:37hs.

⁴⁷ NUCCI, Guilherme de Souza. Manual de Direito Penal. Editora Revista dos Tribunais. São Paulo. 2007. pp. 312-314.

são coletivos e representam o cuidado necessário para o convívio harmônico. Caminhar no escuro exige redobrada atenção e passos pequenos, além de outros mecanismos de navegação que não os olhos, pouco relevantes.

A parcela da sociedade formada pela Internet possui da mesma maneira delinquentes mensuradores dos riscos de serem punidos. E são as inovações trazidas pela tecnologia que dão ao mal intencionado ferramentas para tais ponderações. Destarte, as ferramentas informáticas – como *email*, comunidades virtuais, salas de bate papo, serviços bancários *online* – facilitaram a comunicação e o relacionamento humano, trazendo consigo simbioticamente novas dificuldades.

Apesar de tais e tantos serem os riscos apresentados, o cidadão-usuário não costuma ter capacidade para perceber que a Internet é mera extensão da sociedade. Esta extensão apresenta uma parcela dos mesmos riscos existentes na sociedade material e também novos riscos trazidos por suas facilidades e velocidade. Exemplificativamente, é notório o cuidado que toma um cidadão comum para não conversar com estranhos na vida material; porém em regra tal cautela não é levada à vida virtual, aceitando-se a comunicação desconhecida com certa simpatia e surpresa.

Confrontando a liberdade e a igualdade em grau altíssimo trazido pela sociedade da informação, graças ao anonimato, chega-se a algumas conclusões. Se por um lado goza o usuário comum de ampla possibilidade de relacionamentos, velocidade de navegação e ficam afastadas quaisquer espécies de preconceito, tais características também se aplicam para usuários mal intencionados.

A tranquilidade em navegar em sítios eletrônicos de acordo com curiosidade e interesse sem preocupar-se com reputação ou julgamentos só se dá pelo fato de que o internauta não tem identidade física e não está propenso a avaliações de seus semelhantes.

Conforme apresentado por Heather DiMarco, a rede faz nascer, por exemplo, uma nova sexualidade, tendo-se em vista que as portas de círculos dantes proibidos estão abertas à curiosidade. Diz a pesquisadora da Coventry University da Inglaterra e estudante de desvios

de identidade na cibersociedade⁴⁸ que aqueles que têm insegurança de sua identidade sexual ou simplesmente querem experimentar sexualidades seguras podem utilizar-se da Internet como preparação comportamental para a vida real. Diz, também que *“a tecnologia providencia a ‘máscara’ que faz do proibido permitido e transforma aquilo que é socialmente irrealizável no mundo real em algo que pode ser conseguido virtualmente”*.

É característica da Internet a ampla possibilidade de acesso a quaisquer informações sem o jugo do preconceito ou a política de relacionamento social. O infindável universo de informações disponível virtualmente permite a total exploração com poucos limites, levando garimpeiros virtuais a focarem áreas de interesse e de afinidade, absorvendo cultura direcionada de maneira praticamente ilimitada.

O véu da anonimidade, a velocidade e a farta quantidade de informações é característica essencial da rede. Ocorre que enquanto que na vida real evitar contato com certo tipo de pessoas é relativamente simples – basta não frequentar os mesmos lugares em que tais indivíduos estão –, na Internet a tarefa não é assim tão facilmente contornável, e em grande parte das vezes, aqueles que se gostaria de evitar vão de encontro ao internauta, que por conta do excesso de liberdade, nem sempre tem como evitá-lo.

É também interessante notar o novo potencial lesivo da sociedade virtual. Certamente que nosso Código Penal foi elaborado diante de uma realidade majoritariamente física. Os bens protegidos, em boa parte, são bens tangíveis, materiais. Os raciocínios foram criados diante da criminalidade possível à época e, conforme a sociedade modificou-se, reformas e novidades legislativas surgiram como, por exemplo, violações de propriedade imaterial e à ordem econômica ou tributária.

Ocorre que o mundo material possui limitações, respeita e obedece as regras mínimas da física⁴⁹. Assim, por mais habilidoso que seja um punquista, ele somente poderá

⁴⁸ “The technology provides the “mask “ that makes the impermissible permissible, and transform what it socially unrealizable in the real world into something that can be accomplished in virtual reality”. DIMARCO, Heather. The electronic cloak: secret sexual deviance in cybersociety in DOT.CONNS. Willan Publishing, Devon, 2002. p.65.

⁴⁹ Desconsideraremos no caso a física quântica e da mecânica quântica que demonstra que os átomos não são objetos mas sim tendências e que, portanto, certas partículas podem estar em dois lugares do espaço ao mesmo tempo, naquilo que os estudiosos chamam de emaranhamento quântico. http://www.unicamp.br/unicamp/unicamp_hoje/ju/novembro2006/ju345pag09.html. Acesso em 18.06.08 às

furtar uma carteira por vez por só poder estar em um local no espaço a cada momento.

Na realidade virtual isso ocorre de maneira oposta. Um usuário com conhecimento pode perpetrar instantaneamente ataques a dezenas de milhares de outros usuários, com apenas uma programação, um *email* ou até mesmo um clique.

O fato de não haver regras de conduta interna leva a sociedade virtual a uma tênue situação entre liberdade e temeridade. Por temeridade, entende-se o excesso de liberdade que leva ao desvio, à falta de regras que se mostra prejudicial à sociedade. Certo é que a mera existência das regras informais de etiqueta não serve como desestímulo para condutas por vezes reprováveis.

A falta de controle em qualquer ambiente leva a uma sensação de ambiente corrompido, como uma terra de todos e de ninguém. E é neste cenário que se encontra – e se sente – o delinquente virtual: numa terra sem leis e sem limites como um “*ciber-velho-oeste*”⁵⁰. A mesma liberdade que um usuário comum tem, tem também um usuário com conhecimento para desviar e corromper a finalidade da Internet.

O cidadão virtual comum transita pelas cibervias deparando-se constantemente com outros cidadãos e, por não haver identidade, aparência ou limites sociais, não consegue identificar o bem do mal intencionado. Todos são idênticos na rede e há que se aceitar que por mais delinquentes que haja no mundo real, estes são exceções sociais, prevalecendo o homem de bem que não traz prejuízos ao próximo. Destarte, navega-se na rede partindo-se do mesmo pressuposto: a maioria dos contatos e relacionamentos virtuais é com pessoas de bem, sem intenções prejudiciais e somado a isto está a ideia de que as pessoas acreditam naquilo que preferem que seja verdade.

São palavras de Esther Morón Lerma⁵¹ quanto a cada usuário da rede que:

18:12hs.

⁵⁰ TAYLOR, Paul A.. “*Maestros or misogynists? Gender and the social construction of hacking in DOT.CONs – Crime, deviance and Identity on the Internet*”. Willan Publishing. 2002. p.128

⁵¹ LERMA, Esther Morón. Internet y Derecho Penal: “hacking” y otras conductas ilícitas em la red. In Revista de Derecho y Proceso Penal. Pamplona: Aranzadi Ed. 1999 *apud* ZANELATO, Marco Antonio. Condutas Ilícitas na Sociedade Digital in Direito e Internet. Escola Superior do Ministério Público de São Paulo. Ano II, nº IV. São Paulo. 2002. p. 170

“Cada indivíduo é potencialmente um emissor e um receptor em um meio qualitativamente diferenciado, em que todos se comunicam com todos. Os internautas não se localizam principalmente por seu nome, posição social ou situação geográfica, mas a partir de centros de interesses. É um mundo virtual segregado pela comunicação.”

Acredita-se que ataques diretos e com o uso da tecnologia aproveitando-se da normal ignorância ou do menor conhecimento do usuário-alvo chegam a ser verdadeiros recursos que dificultam ou tornam impossível a defesa da vítima, posto que o meio é por si obscuro e de difícil compreensão. Se atacado, por exemplo, o usuário não sabe de onde vem a invasão, quem o invade, porque o invade, o que quer e sequer se houve ou não modificação ou estrago em seu sistema.

Destaque-se que o crime informático é uma espécie de crime especial, de colarinho branco porquanto praticado por pessoas educadas e grupos privilegiados⁵², e que assumirá, na opinião de especialistas, precipuamente a liderança dentre os crimes no mundo em pouquíssimo tempo⁵³.

Delinquentes virtuais, então, não são como os estereotipados na sociedade real: não frequentam classes baixas necessariamente, normalmente não precisam cometer infrações penais para sobreviverem e virtualmente aparentam tanta periculosidade quanto qualquer usuário: nenhuma.

Não há como identificar pelo IP de alguém⁵⁴ antecedência criminal, intenção ou ofensividade. Somos todos igualmente nocivos e igualmente perigosos na rede e qualquer um pode desviar seu comportamento com a mesma facilidade e naturalidade com que envia um cartão virtual.

⁵² ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática. Editora Juarez de Oliveira, São Paulo, 2006, p. 11.

⁵³ “PF: em 10 anos, 90% dos crimes serão pela Internet” em <http://noticias.terra.com.br/brasil/interna/0,,OI2948600-EI10651.00.html>. Acesso em 17.06.2008 às 16:24hs.

⁵⁴ A expressão correta não seria “IP de alguém”, mas sim “IP de uma máquina que algum usuário está utilizando” tendo-se em consideração que tal numeral não corresponde a uma pessoa mas sim a uma conexão e que, por sua vez, requer um aparato informático.

Diante disso, acredita-se certo o entendimento de que os direitos e vantagens da tecnologia são garantidos integralmente a qualquer um, numa liberdade em sentido amplíssimo. A variância estaria, pois e somente, na intenção do agente.

Nesta etapa do desenvolver do raciocínio, cabe apresentar a noção de *hacker* e a forma classificatória criada pelos próprios, nas figuras do *White Hat*, do *Grey Hat* e do *Black Hat*.

As expressões acima citadas referem-se respectivamente às ideias de “chapéu branco”, “chapéu cinza” e “chapéu preto”, três expressões cunhadas na própria rede para diferenciar as espécies de *hackers* existentes.

O termo “*hacker*” tem uma ampla variedade de interpretações; contudo, neste trabalho entenderemos como *hacker* o indivíduo, usuário da informática e da rede mundial de computadores, com conhecimento acima da média, e que, por tal capacidade, tem potencialidade para programar, modificar *softwares*, invadir sistemas, encontrar brechas de segurança, etc. Nas palavras de Orly Turgeman-Goldschmidt, são portadores de desvios positivos que, por sua vez, são atitudes que potencialmente podem gerar desconforto e prejuízo alheios mas que se mantêm sob controle pela ausência de *dolus malus*⁵⁵.

Desta forma e partindo dessas premissas, imprescindível compreender a diferenciação dada pelos *hackers* quanto à intenção lesiva⁵⁶. Os “chapéus brancos” seriam os *hackers* sem intenção de violar bens jurídicos mas tão somente detectar “*bugs*” e falhas de segurança e auxiliarem no conserto e melhoria do programa ou sistema de segurança; seriam os “*hackers do bem*”. Em total contrapartida estariam os “chapéus pretos”, conhecedores dos meandros informáticos mas que somente utilizam tal conhecimento para práticas lesivas que trazem prejuízos reais para os ofendidos; seriam os “*hackers do mal*” ou, para alguns, os “*crackers*”. Finalmente, os “chapéus cinzas” seriam aqueles que hora praticam atitudes solidárias e cordatas e hora praticam lesões a bem jurídicos.

⁵⁵ TURGEMAN-GOLDSCHMIDT, Orly. The Rhetoric of Hackers’ Neutralizations. In Crimes of the Internet, Pearson Prentice Hall, New Jersey, 2008, pp. 329-332.

⁵⁶Na mesma linha de raciocínio FINCH: “Therefore, just as the Internet offers possibilities for users to develop new facets of their personality, it also confers the opportunity to develop negative, i.e. criminal, characteristics without the feeling of insecurity or vulnerability that would be attached to analogous behavior in real life”. FINCH, Emily. Op. cit., p. 41

Foram, pois, os próprios expertos quem se preocuparam acerca da necessidade de se ponderar o elemento subjetivo do tipo nos crimes informáticos⁵⁷. Todavia, ao invés de buscarem a racionalidade da obediência ao Princípio da culpabilidade, preferiram rotular *a priori* as espécies de agentes causadores de condutas, criando uma espécie de padrão e até mesmo uma presunção de dolo para certos tipos de delinquentes.

Pode-se certamente concluir que a rede criada pelos meios informáticos obedece regras como qualquer segmento social. Se há formas de se comportar com educação e etiqueta na rede, seguro é que tal meio representa parcela da própria sociedade e exige os mesmos cuidados.

Eric Arthur Blair, utilizando-se do pseudônimo George Orwell, publicou em 1949 um romance revolucionário denominado “1984” em que previa a existência de um Estado totalitário denominado Grande Irmão (*Big Brother*). O regime seria capaz de ver tudo, saber de tudo e controlar todos os cidadãos desde o nascimento. Buscou, no romance, alertar sobre os riscos da sociedade moderna, mais focado nos riscos dos regimes totalitários da época (Hitler, Mussolini, etc), mas acabou por retratar algo próximo com o que a sociedade atual é com a informática e a Internet.

No livro, o regime cria a “Novilíngua”, um novo idioma construído para fazer com que os cidadãos não pudessem – por não conhecer palavras – criticar o regime totalitário vigente, excluindo-se certas expressões e, assim, controlando inclusive o pensamento dos cidadãos.

Respeitadas as devidas proporções, a tecnologia fez-se imprescindível na vida das pessoas e a cada dia mais faz com que os indivíduos tornem-se escravos dela, além de ter feito surgir um dialeto próprio. Esquecer o celular em algum lugar ou ficar sem conexão com a rede torna-se pesadelo⁵⁸ porquanto o mundo informático adicionou à vida das pessoas uma nova

⁵⁷ Não se pode olvidar, porém, que a Convenção de Budapeste, de 23 de novembro de 2001, estabeleceu o dolo como elemento subjetivo dos crimes informáticos e, em alguns casos, até mesmo o dolo específico como no enriquecimento ilícito ou na indisponibilidade de sistemas informáticos. ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática. Editora Juarez de Oliveira. 2006. p. 29

⁵⁸ A ansiedade que surge pela perda de conexão, pela indisponibilidade dos aparatos ou pelo travamento de um sistema já se tornou tema de estudos sobre a ansiedade, cunhando o termo *technology-related anxiety*, de acordo com Richard Saul Wurman em seu livro Ansiedade de Informação. Fonte: Revista Superinteressante, novembro 2008, Editora Abril, p. 72.

utilidade, imprescindível, agregando-se irreversivelmente aos processos diuturnos. A utilidade da nova ferramenta supera seu próprio valor.

Também, a evolução tecnológica fez com que as pessoas passem a ser encontradas em praticamente todo o lugar através de comunicadores instantâneos, mensagens de texto, telefonia celular, tecnologia GPS e até mesmo câmeras de segurança disseminadas. O meio informático, por sua vez, criou uma linguagem própria, ora criando, ora reduzindo palavras, e até mesmo nacionalizando expressões em língua inglesa⁵⁹.

A informática em si acaba por estar cada dia mais presente na vida do cidadão, tornando-se um nicho de exploração constante das empresas, que vigiam incansavelmente os usuarios por serem potenciais consumidores constantes, monitorando cada clique da rede⁶⁰.

Apesar de existirem regras internas nos círculos sociais restritos como, por exemplo, uma cela de presídio ou entidade familiar, tais formas de conduta têm limites para seu estabelecimento nas regras gerais.

Internamente, pode o chefe de uma célula ditar horário para repouso, obrigatoriedade de higiene e divisão do espaço individual; mas não pode haver violação quanto a bens jurídicos protegidos macro socialmente. O pai pode impor limites ao filho, mas não pode lesioná-lo ou cercear sua liberdade e educação. Um superior hierárquico pode dar ordens, mas jamais violar a razoabilidade e impor que seu subalterno viole direitos alheios em ilegalidade.

Em suma, a realidade virtual criada pelos meios informáticos termina por igualar-se em muito nos aspectos comuns. A visita a *sites* desconhecidos exige cuidados da mesma forma como a locais físicos. Enquanto que se aprende na infância que não se deve conversar com estranhos, o mesmo pode ser levado à realidade virtual.

Claus Roxin, desde os idos de 1970, com ideias pós finalistas, trouxe pensamentos

⁵⁹ O dicionário HOUAISS, por exemplo, já traz expressões como “clicar”, “deletar”, “mouse”, “escanear” dentre outras.

⁶⁰ Especialmente através de *Spywares*, como veremos adiante em capítulo próprio para os crimes informáticos. A importância da rede para a exploração comercial das empresas pode ser notada acessando-se o programa *Second Life*, um simulador de vida em que o usuário cria um personagem e o conduz e administra em situações da vida comum, com alguns recursos a mais. Por conta do sucesso do programa e a visibilidade que o meio virtual passou a ter, as empresas investiram em publicidade maciça nesse novo ambiente, para que suas marcas fossem fixadas nas mentes dos consumidores-usuários. <http://secondlife.com/>. Acesso em 15.12.08 às 13:00hs.

acerca de uma teoria funcionalista num raciocínio do risco dentro da sociedade, assim trazendo novo elemento revolucionário para o pensamento do crime.

Em linhas gerais, a ideia é a de que o ser humano da sociedade pós-industrial, vive numa sociedade insegura, de riscos constantes e necessários, e que tais elementos devem ser levados em conta para se concluir se há ou não tipificação de um crime.

Assim, o fenômeno da modernização (científica e tecnológica) traz para a sociedade transformações, grande parte das vezes de proporções muito superiores à capacidade de adaptação e de controle jurídico. Como bem afirma Anthony Giddens, não há confiança e tranquilidade na sociedade atual, uma vez que a própria ciência contradiz as verdades por si mesma afirmadas, apresentando fatos que muitas vezes se negam, colocando o cidadão em dificuldades⁶¹.

Isto posto, a ciência tecnológica-informática é certamente a que traz maiores revoluções e em velocidade mais assustadora⁶². Com isso, o que se quer trazer para a exposição é o fato de que a criação de um ambiente eletrônico, e até mesmo computacional e virtual, é uma evolução da modernidade e que, assim, sem fugir à regra, traz em si insegurança, visto que sua regulamentação é incapaz de acompanhar o evoluir da tecnologia⁶³. Assim, é certo que a Internet gera insegurança tanto social, quanto econômica e jurídica porquanto em modificação constante, gerando assim ciclos de revolução de conceitos.

A sociedade informática, pois, deve ser ainda vista como uma sociedade de risco “*sui generis*” pois que além dos riscos previsíveis, controláveis e mitigáveis da sociedade comum, ainda tem a variante da gigantesca capacidade de mudança inerente à tecnologia da informação.

Se por um lado os objetos e serviços desenvolvidos na sociedade material apresentam

⁶¹ *Apud* SALVADOR NETTO, Alamiro Velludo. *Tipicidade Penal e Sociedade de Risco*. São Paulo. Quartier Latin. 2006. p. 82.

⁶² A Lei de Moore é o exemplo mais emblemático. Sem prazo para cessar, ela enuncia que a cada 24 meses, a capacidade de processamento dos computadores dobra, enquanto os custos permanecem constantes. Ressalte-se que o postulado está em vigor há mais de 30 anos.

⁶³ “*Com o avanço dos meios tecnológicos, novos riscos sociais foram postos, modificando por completo o dia a dia dos homens. Essa nova fase da vida em sociedade dos tempos chamados pós-modernos tem sido profundamente questionado por filósofos, sociólogos e juristas*”. SILVEIRA, Renato de Mello Jorge. *Direito penal supra individual – interesses difusos*. São Paulo. Editora Revista dos Tribunais. 2003. p. 17

riscos, é notório contudo, que boa parte de tais riscos, por serem palpáveis, são mais possivelmente identificáveis, pois que a materialidade implica limites e respeito a alguns postulados da física.

No que tange ao crime informático, o risco torna-se dilatado. As prospecções do futuro, o vulto tomado pela tecnologia e os recursos existentes no presente levam-nos à ideia de que, o uso da informática é hábil para o cometimento de qualquer conduta que viole bens jurídicos protegidos.

Para conseguir trazer o conceito de sociedade de risco, natural exigir-se o raciocínio da imputação objetiva que irá, pois, numa ótica penal, avaliar quais condutas do meio informático são ou não toleradas pela sociedade. Irá, também, verificar se a conduta poderá ser imputada a alguém diante da automação dos recursos e da ideia de responsabilidade penal imanente em nosso ordenamento jurídico.

Fundamental será que com base nesta nova sociedade, verifique-se se o agente criou ou incrementou o risco tolerável pela sociedade e, em incrementando, acabou por realizar tal risco num resultado concreto, dentro daquilo previsto na norma existente ou em uma norma que porventura venha a reger novos bens jurídicos.

A análise da conduta passa a estar imersa em toda uma contextualização social complexa. Mas torna-se impossível que tais ponderações ocorram sem que se tenha claro o conceito de crime informático, a forma como a doutrina o classifica, suas principais modalidades, quais bens jurídicos ainda exigem conceituação e proteção e quem está envolvido direta e indiretamente nessa nova tendência social.

OS DELITOS INFORMÁTICOS

“Informação é em si mesmo um poder, um homem pode tanto quando sabe, o homem é aquilo que sabe” (Francis Bacon)

ASPECTOS PRELIMINARES

Para iniciar qualquer estudo acerca do papel da vítima nos crimes informáticos, é mister que primeiramente se delimite o que seriam os referidos delitos, suas características e particularidades, bem como a forma de classificar tais delitos e os bens jurídicos envolvidos.

A expressão crimes informáticos não é adotada de maneira uniforme pela doutrina, que apresenta outras nomenclaturas para o mesmo estudo, quais sejam, exemplificativamente *“crimes da era da informação”, “crimes mediante computadores”, “crimes cibernéticos”, “cibercrimes”, “crimes de computador”, “crimes eletrônicos”, “crimes tecnológicos”, “crimes digitais”, “crimes hi tech”, “tecnocrimes”, “netcrimes”, “crimes virtuais”, “crimes da tecnologia da informação”*⁶⁴ e até mesmo *“e-crimes”*.

Nossa opção pelo termo se dá com base no intuito amplo de tratar de uma criminalidade que não está limitada às tecnologias existentes, nem limitada à Internet ou aos computadores, mas sim aquelas condutas que vão utilizando um novo ferramental conforme evolui o ser humano e a ciência – seja a nanotecnologia, a telefonia, a computação, a robótica ou qualquer outro ramo que crie aparatos facilitadores das tarefas diuturnas. Assim, e tendo-se em vista a tendência de integrarem-se aparelhos e se retirar do ser humano tarefas e funções, destinando à automação uma grande gama de ações, optou-se pela informática como apoio.

A informática é o ramo do saber que estuda o tratamento da informação através da utilização de computadores e outros dispositivos de tratamento de dados⁶⁵ como celulares, *palmtops*, etc.

Destarte, por conta de a sociedade pós-industrial desenvolver-se com forte viés para a cultura da informação e comunicação, inclusive ampliando a cada dia os estudos da

⁶⁴ JAISHANKAR, K. Space Transition Theory of Cyber Crimes in Crimes of the Internet. Pearson Prentice Hall. New Jersey, 2008, p. 286.

⁶⁵ Dicionário Houaiss da Língua Portuguesa – versão eletrônica. Disponível em <http://houaiss.uol.com.br/busca.jhtm?verbete=inform%Etica&stype=k>. Acesso em 31.01.08 às 12:53

Tecnologia da Informação (TI) – o conjunto de atividades providas por computadores – que se destaca como serviço de maior expansão e destaque no setor laborativo⁶⁶, a nomenclatura “informática” será privilegiada.

A revolução industrial girou em torno de uma sociedade lastreada em recursos finitos, extraídos da natureza em sua grande maioria, e transformados pelo homem. A sociedade em que se encontra a informática, entretanto, denominada sociedade pós-industrial (ou sociedade informática, sociedade do conhecimento, sociedade tecnizada ou sociedade em rede), existe embasada e organizada em torno da informação. Ocorre que enquanto que os recursos daquela revolução são esgotáveis, a informação é infinita e está em constante crescimento.

Com base em tal premissa, é mister concluir que, na sociedade moderna e futura, informação é um ativo e, pois, sustenta um valor econômico, gera riqueza e gera poder para aqueles que a detém, bem como para aqueles que sabem manejá-la e comercializá-la⁶⁷.

Conforme evoluímos, mais e mais deixamos que a tecnologia informática tome espaço em nossas vidas. O ferramental capaz de criar e armazenar documentos leva-nos a um momento em que fichas médicas, informações bancárias, planilhas de custos, projetos, fotos, filmes, livros, enfim, uma gama imensa de informações transforma-se em *bits* e ficar disponível para consulta e utilização.

Até sem saber, os caminhos feitos dentro da rede, as aquisições feitas com cartão de crédito ou pelo celular, as conversas que ocorrem com outros usuarios e até mesmo senhas e dados pessoais vagam pela rede, num ambiente em que cada informação importa.

Segredos industriais criados e armazenados como arquivos eletrônicos podem valer milhões⁶⁸, assim como uma próxima edição de um livro⁶⁹, e tais patrimônios não podem

⁶⁶ De acordo com o Jornal O Globo, a Tecnologia da Informação (TI) na América Latina terá crescimento em torno de 13% em 2008, com consumo de cerca de US\$ 48 bilhões. disponível em http://oglobo.globo.com/tecnologia/mat/2008/01/17/mercado_de_ti_vai_crescer_13_em_2008_na_america_latina_afirma_idc-328073912.asp. Acesso em 31.01.08 às 13:55hs.

⁶⁷ ZANELATO, Marco Antonio. Condutas Ilícitas na Sociedade Digital *in* Direito e Internet. Escola Superior do Ministério Público de São Paulo. Ano II, nº IV. São Paulo. 2002. p. 177

⁶⁸ Veja, por exemplo, os dados contidos em notebooks da Petrobras, furtados, e que continham dados referentes a novos poços a serem perfurados e novos locais de exploração de petróleo, sendo que tais informações poderiam valer bilhões de dólares. Em <http://portal.rpc.com.br/gazetadopovo/economia/conteudo.phtml?tl=1&id=737772&tit=Dados-sigilosos-sobre->

sequer ser lidos sem o auxílio da informática.

O crime informático deve ser avaliado sob diferentes perspectivas por conta de suas peculiaridades.

As regras comumente utilizadas para definir condutas e regras a sociedade levaram em conta a ideia de Estado como sendo uma instituição composta cumulativamente por população, território e governo⁷⁰, todos presentes e tangíveis. As regras penais e outras estavam alicerçadas no conceito de ambiente físico, no qual crimes do mundo real ocorriam, e que tem como pilstras a (i) proximidade, a (ii) escala, (iii) o constrangimento físico e (iv) padrões⁷¹.

De acordo com o Direito Penal do mundo físico, o ofensor e a vítima estão necessariamente próximos quando o fato típico ocorre, sendo, pois, impossível o cometimento de, p. ex., um estupro sem contato, portanto entre pessoas distantes.

A criminalidade em tal situação é entre singulares e aquele que comete o fato (ou minimamente o tenta, sem atingir o exaurimento) necessariamente deverá dispende algum tempo na preparação de um crime como, por exemplo, um roubo a bancos. Há necessidade de planejamento, análise, ponderação, visita ao local, e durante tal processo pode o delinquente ser visto e notar-se maneira suspeita em seu comportamento. Há, na criminalidade real, alto risco porquanto se exige movimento físico e contato.

Com isso, é de se dizer que a criminalidade do mundo real é mais simples de se combater uma vez que o agente criminoso está limitado no espaço e comete apenas um crime por vez. Cometido o fato, o crime real tem local precisado e a polícia passa a agir *in loco*, focada no ambiente em que houve o fato jurídico, naquele segmento social.

[descobertas-da-Petrobras-sao-roubados](#). Acesso em 30.07.08 às 18:30hs

⁶⁹ Como é o caso da bilionária saga literária de Harry Potter em que sua autora, J. K. Rowling, foi obrigada a escrever em webcafés e LAN houses para evitar que porventura qualquer informação dos futuros exemplares fosse conhecida por qualquer leitor antes do lançamento do livro, o que geraria alta cifra de prejuízos. Em <http://noticias.uol.com.br/ultnot/internacional/2006/12/21/ult2242u1325.jhtm> Acesso em 25.08.08 às 11:44hs.

⁷⁰ MALUF, Sahid. Teoria Geral do Estado. Editora Saraiva. 24a Edição. São Paulo. 1998. pp. 23-28.

⁷¹ Brenner, S. Toward a criminal Law of cyberspace: distributed security. Boston University Journal of Science & Technology Law, 10 (2). 2004 *apud* BRENNER, Susan W. Cybercrime: re-thinking crime control strategies. Crime Online. Willan Publishing, Devon, 2007, p. 14.

Analisar-se parte do artigo 6º do Código de Processo Penal e se percebe a forma como a legislação foi construída nos idos de 1941 no que toca à realidade dos crimes, objetivando o trabalho da autoridade policial pois que:

“Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; [\(Redação dada pela Lei nº 8.862, de 28.3.1994\)](#) [\(Vide Lei nº 5.970, de 1973\)](#)

II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; [\(Redação dada pela Lei nº 8.862, de 28.3.1994\)](#)

(...)

VI - proceder a reconhecimento de pessoas e coisas e a acareações;”(grifos nossos)

Não há dúvida que parte de tal legislação não tem aplicabilidade alguma naqueles delitos em que não há local, nem palpabilidade⁷². Conforme adiante, dados sequer podem ser considerados coisa.

Não raro dizer que a criminalidade do mundo real segue padrões analisáveis como locais de maior ocorrência, concentração de delitos em regiões mais demográficas, maiores índices em regiões com pior iluminação, entre tantos⁷³, permitindo-se, pois, intervenção dirigida da segurança pública e políticas criminais de prevenção pontuais.

O crime informático, por sua vez, tem características tão próprias, que boa parte dos requisitos acima elencados são inaplicáveis. Tal categoria de crimes dispensa o contato físico

⁷² Note-se que os vestígios do crime informático, por sua inerente imaterialidade, são imediatamente frios e sujeitos a desaparecimento, e a polícia dificilmente terá acesso imediato às evidências. BRENNER, Susan W. Cybercrime: re-thinking crime control strategies. In Crime Online. Willan Publishing. 2007. p.17.

⁷³ Outros exemplos poderiam ser o uso de armas de fogo nos crimes contra a vida e de roubo, a maior concentração de tráfico de entorpecentes em regiões afastadas e de menor desenvolvimento social.

entre vítima e ofensor, não exige grandes preparos como visitação prévia de local para o cometimento do fato, ocorre em um ambiente sem povo, governo ou território, não implica aparentemente em altos riscos, não gera sensação de violência e não há padrões para seu acontecimento.

O criminoso informático pode cometer mais de uma conduta lesiva ao mesmo tempo, estando em diversos lugares simultaneamente, e conta com a vantagem de haver poucos profissionais de segurança pública capacitados para investigar sua ação, analisar as provas e os indícios. Sem contar a vantagem de o agente não fazer qualquer esforço e agir de forma transnacional com facilidade ímpar.

O fato de os crimes informáticos serem discretos e silenciosos e por conta de a população em sua maioria não denunciar a vitimização em tais casos, faz com que a chamada cifra negra de tal ramo do Direito Penal seja elevada, clamando por métodos de avaliação suplementares como os *victimization studies*⁷⁴ (pesquisas de vitimização)

A falta de comunicação dos crimes informáticos se dá por três razões principais. A primeira é o acanhamento do ofendido que crê que ser lesado através da informática implica em sensação de vulnerabilidade, fraqueza e incapacidade em dominar a tecnologia, gerando, portanto, uma resistência em expor-se. A segunda, aplicável exclusivamente às pessoas jurídicas – especialmente instituições bancárias, lojas virtuais e companhias de seguro –, é o receio de, ao denunciar, gerar uma perda de confiança dos consumidores em utilizarem-se da informática para contratar⁷⁵. A terceira é a falta de crédito dado ao poder público para obter

⁷⁴ De acordo com Pablos de Molina, tais pesquisas são fontes secundárias e não oficiais de informação e constituem de questionários estruturados com perguntas focadas na arguição de cidadãos acerca de ter sido vítima de delito, ter denunciado o fato à autoridade policial e o *modus operandi* do infrator. Assim, aproximam-se do descobrimento do volume real da criminalidade. PABLOS DE MOLINA, Antonio Garcia. *Criminologia*. 5ª Edição. Editora Revista dos Tribunais. 2006. pp. 46-47.

Um exemplo interessante de pesquisa de vitimização foi conduzida por Tony Krone and Holly Johnson e denominada “*Internet purchasing: perceptions and experiences of Australian households*”, publicada na Revista Eletrônica *Trends and Issues* do Instituto Australiano de Criminologia do Governo da Austrália em fevereiro de 2007, disponível em <http://www.aic.gov.au/publications/tandi2/tandi330.html>. Acesso em 18.12.08 às 20:49hs.

⁷⁵ Aqui cabe citarmos as instituições bancárias que costumeiramente desencorajam seus clientes vítimas de crimes informáticos a registrarem ocorrência, para evitar o surgimento de estatísticas que exponham a vulnerabilidade de suas plataformas virtuais. A geração de sensação de insegurança que poderia ser gerada no mercado de Internet banking levaria, pois, a um descrédito que levaria a um aumento do custo operacional de tais instituições tendo-se em vista que os usuarios migrariam de volta para o atendimento pessoal nas agências exigindo-se, pois, mais funcionários contratados.

uma punição razoável somada ao fato de que a reparação da vítima dificilmente ocorre⁷⁶.

Some-se ao acima descrito o fato de que ainda que se consiga perseguir o agente delinquente e encontrá-lo, há ainda assim grande possibilidade de mais de uma nação estar envolvida e haver conflito entre leis processuais e penais, por exemplo, tornando-se difícil o sequestro dos suportes de dados, a extradição do(s) indivíduo(s)⁷⁷ (mormente por ausência de previsão legislativa do tipo) e até mesmo não haver delegacias especializadas e juízos preparados para procederem corretamente à apuração dos fatos nem peritos suficientes com conhecimento.

Por hora, consenso é que a nova criminalidade tende a ser praticada através da tecnologia desenvolvida especialmente para o trato da informação de maneira automatizada, ou seja, através de aparelhos cada dia mais sofisticados que se utilizam da ciência da informática, como *notebooks*, computadores, aparelhos de telefonia móvel, tocadores de música, etc.

Ainda que não haja um consenso internacional acerca de uma definição, de acordo com os trabalhos da Organização para Cooperação e Desenvolvimento Econômico (OCDE) iniciados em 1989 “*considera-se abuso informático qualquer comportamento ilícito, aéctico ou não autorizado relacionado ao processamento automático e à transmissão de dados*”⁷⁸. Em verdade, o trabalho de aproximar-se da problemática dos crimes informáticos foi continuado pelo Comitê Europeu para Problemas Criminais do Conselho da Europa que não chegou a uma definição formal de crimes informáticos (*computer-related crimes*⁷⁹, na expressão original),

⁷⁶ Nesse sentido, STANGELAND, Per. Criminología realista y El problema de las víctimas in *Problemas criminológicos em las sociedades complejas*. Universidad Publica de Navarra. Espanha, 2000, p. 142.; também, CÂMARA, Guilherme Costa. Op. cit. pp. 93-94.

⁷⁷ São os requisitos para a concessão da extradição no Brasil, segundo Guilherme de Souza Nucci, “1º) *exame prévio do Supremo Tribunal Federal (art. 102, I, g, CF)*; 2º) *existência de convenção ou tratado firmado com o Brasil ou oferecimento de reciprocidade (arts. 49, I e 84 da CF)*; 3º) *existência de sentença final condenatória*; 4º) *ser o extraditando estrangeiro (art. 5º, LI, CF)*; 5º) *o fato imputado deve constituir crime perante a lei brasileira e a do Estado requerente*; 6º) *a pena máxima para o crime imputado ao extraditando deve ser a privativa de liberdade superior a um ano*; 7º) *o crime imputado ao extraditando não pode ser político ou de opinião (art. 5º, LII, CF e art. 77, VII, do Estatuto do Estrangeiro)*; 8º) *o extraditando não pode estar sendo processado nem pode ter sido condenado ou absolvido no Brasil*; 9º) *o Brasil tem que ser incompetente para julgar a infração*; 10º) *o extraditando, no exterior, não pode ser submetido a tribunal de exceção e 11º) não pode estar extinta a punibilidade pela prescrição*.”. NUCCI, Guilherme de Souza. Manual de Direito Penal. 3ª Edição. Editora Revista dos Tribunais, São Paulo, 2007, pp. 123-125.

⁷⁸ Computer-related Crime (Recommendation n. R. 89 (9)). Strasbourg, Council of Europe, 1990, p. 13

⁷⁹ Crimes relacionados com computador.

deixando que cada país adaptasse uma classificação que lhe fosse mais funcional de acordo com seu sistema legal.

A ciência do Direito Penal, não se contentando com a expressão “abuso” trazida pela OCDE foi obrigada a buscar uma definição mais aproximada com seus Princípios e teorias. Diante disto, diversos doutrinadores⁸⁰ aventuraram-se em buscar respostas.

Quiçá um dos primeiros a definirem tal espécie foi Klaus Tiedemann que a apresentou como sendo todos os atos antijurídicos, segundo a lei penal vigente, realizados com o emprego de um equipamento automático de processamento de dados⁸¹.

Marco Aurélio Rodrigues da Costa, por sua vez, em conceituação mais específica, aponta que crime de informática é todo aquele procedimento que, utilizando-se de um sistema de processamento de dados, atenta contra os dados que estejam armazenados, compilados, sejam transmissíveis ou em transmissão⁸².

Optou-se inicialmente pela definição mais abrangente dada por Ivete Senise Ferreira, que apresenta delito informático como sendo a ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão⁸³.

As definições da expressão podem trazer desvantagens tendo-se em vista seu caráter estático fulcrado na positivação da conduta, o que, especialmente diante de uma criminalidade

⁸⁰ Outras definições de João Marcello Araujo Junior (“conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática”), Marco Aurélio Rodrigues da Costa (“todo aquele procedimento que atenta contra dados, que o faz na forma em que estejam armazenados, compilados, transmitidos ou em transmissão”) e Gustavo Correia (“crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico”) in Carla Rodrigues Araújo de Castro, *Crimes de Informática e seus Aspectos Processuais*, 2ª Edição, Lumen Juris, 2003, Rio de Janeiro, pp. 8-9

⁸¹ TIEDEMANN, Klaus. “Criminalidad mediante computadoras”. Poder Economico y Delito. Barcelona. Editorial Ariel S.A., traduzido por Amélia Mantilla Villegas, 1985, p. 122 *apud* LUIZ GUILHERME MOREIRA PORTO - “Fraude Informática”, ob. coletiva Comércio Eletrônico (coordenadores Ronaldo Lemos da Silva Júnior e Ivo Waisberg), co-edição IASP e Editora RT, São Paulo, pp. 275-276. Também ROSSINI, Augusto. Informática, telemática e Direito Penal. Memória Jurídica Editora, São Paulo, 2004, p. 114.

⁸² COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. Em <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em 31.12.08 às 13:05hs; e *apud* ROSSINI, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. Memória Jurídica Editora, São Paulo, 2004, p. 119-120.

⁸³ Ivete Senise Ferreira, *A Criminalidade Informática, in Direito & Internet – Aspectos Jurídicos Relevantes*, EDIPRO, 2000, p.210.

fulcrada na tecnologia da informação – altamente dinâmica e mutável –, pode levar a superações rápidas levando-se ao afastamento frente à realidade.

Contudo, mais ampla que é tal definição, permite que se obtenha uma classificação, que aponta que há duas maneiras de se cometer um crime informático: a) atacando o processamento automático de dados ou sua transmissão qualquer que seja o intuito do agente; ou b) pela utilização de processamento automático de dados ou sua transmissão⁸⁴ como ferramenta.

A partir deste entendimento, conclui-se que na criminalidade informática, os bens jurídicos atacados serão ou (a) um sistema de processamento de dados/ a transmissão de dados, ou (b) qualquer outro bem jurídico, desde que especificamente violado pelo intermédio do recurso do processamento automático de dados ou sua transmissão.

No primeiro caso, há dolo específico de violação de um bem informático; a violação informática é o fim almejado. No segundo caso, o dolo não guarda necessária relação com a informática pois que o bem atingido não será necessariamente informático, mas, em contrapartida, será a informática responsável pelo atingimento do resultado como meio.

Em tempo, independentemente da definição para crimes informáticos, para melhor explicar o tema, diversas classificações também surgiram ao longo do recente estudo. Algumas classificações levaram em conta os bens jurídicos, as condutas, e até mesmo a forma de cometimento, dentre as quais se destaca algumas.

Ulrich Sieber dividiu os delitos informáticos em três grupos, levando em conta o bem jurídico afetado: a) os delitos econômicos, que se subdividem em a1) fraude de manipulação de dados em sistema de processamento de dados; a2) espionagem de dados e pirataria de programas; a3) sabotagem; a4) furto de serviço ou furto de tempo; a5) acesso não autorizado a sistema de processamento de dados; e a6) uso de computadores para crimes empresariais; b) os delitos contra direitos individuais, que se subdividem em b1) uso incorreto de informações;

⁸⁴ Hervé Croze e Yves Bismuth, *Droit de l'Element de Droit à l'Usage des Informaticiens*. Economica, Paris, 1986, p. 207, *apud* Ivete Senise Ferreira. *A Criminalidade Informática. In Direito & Internet – Aspectos Jurídicos Relevantes*, EDIPRO, 2000, pp. 214-215; Rigorosamente, também, as características podem co-existir e simultaneamente haver crime contra o processamento automático de dados ou transmissão perpetrado com o uso de outro meio de processamento de dados ou transmissão, sendo os crimes de aparato contra aparato.

b2) obtenção ilegal de dados e posterior arquivo das informações; b3) revelação ilegal e mal uso de informações; e c) os delitos contra direitos supra individuais, divididos em c1) ofensas contra interesses estaduais e políticos, e c2) crimes contra a integridade humana⁸⁵.

Carlos M. Romeo Casabona, por sua vez, categoriza as infrações de acordo com a forma de cometimento, sendo, pois, os delitos de a) manipulação de entrada de dados (*input*)⁸⁶; b) manipulação no programa; c) manipulação de saída de dados (*output*) e d) manipulação à distância⁸⁷.

No que se refere à forma de cometimento, um maior número de doutrinadores se debruçou e anui em parte com a divisão proposta por Senise a partir do estudo de Hervé Croze e Yves Bismuth, qual seja, a de delitos informáticos próprios e delitos informáticos impróprios. Os primeiros seriam aqueles em que bens jurídicos novos (ou que necessitam adaptação legislativa) são o alvo de violação. Os impuros seriam os crimes cometidos pelo uso do ferramental informático como forma de opção livre do delinquente, mas que não implicam em novos raciocínios jurídico-penais.

Destarte, o que se tem é que os crimes informáticos podem ser amplamente compreendidos dividindo-se (i) o meio tecnológico como alvo da conduta ou (ii) o meio eletrônico como ferramenta para conseguir obter a finalidade delituosa.

Em nossa concepção, porém, são três as formas de se perpetrar aquilo que se denomina delito informático:

1. Violando-se o meio informático em si, em seus elementos, fazendo uso de ferramentas comuns;
2. Utilizando-se do meio informático como instrumento para atacar-se outro bem

⁸⁵ *Apud* ROSSINI, Augusto. Informática, Telemática e Direito Penal. Memória Jurídica Editora. São Paulo. 2004. pp.114-115.

⁸⁶ Entrada de dados seria o ato de alimentar um sistema com informações antes da obtenção de qualquer resultado, enquanto que saída de dados seria o resultado obtido da alimentação de informações. Desta forma, uma fraude em nível de input seria a inserção de dados deturpados ou a inserção de dados incorretos ou modificados. Em contrapartida, fraude em nível de output seria a produção artificial de resultado diverso do correto por manipulação do sistema ou da etapa de resultados.

⁸⁷ *Apud* ROSSINI, Augusto. Informática, Telemática e Direito Penal. Memória Jurídica Editora. São Paulo. 2004. pp.116.

jurídico; e

3. Violando-se o meio informático em si, em seus elementos, mas utilizando-se para isso exclusivamente do meio informático (portanto não ferramentar comuns).

Exemplificativamente, o primeiro caso, seria o uso de um martelo para destruir o suporte de dados, seja um disco rígido, seja um DVD, seja a própria máquina. Neste caso, se está diante de um crime comum, de dano, em que o alvo é físico, mas acaba indiretamente implicando em violação aos dados e ao sistema de processamento.

O segundo caso seria o envio de uma mensagem eletrônica para um usuário, pedindo que acredite em uma história e deposite uma quantidade de dinheiro para ajudar uma pessoa que precisa de um transplante de medula. Aqui, o crime praticado viola o bem jurídico patrimônio e o delinquente opta pelo uso de sistemas de informática em detrimento a outros meios, ardilosamente, para convencer o destinatário da mensagem a auferir-lhe vantagem patrimonial.

A terceira hipótese seria, por exemplo, a inserção de um código malicioso (formado de *bits*, portanto intangível) no computador de um escritório, a partir de um *notebook*, capaz de impedir que os usuários acessem arquivos fundamentais.

Pela classificação mais abrangente considerar-se-ia tanto o primeiro quanto o terceiro exemplos como sendo de delitos informáticos próprios. Isso levaria a uma abrangência de crimes essencialmente diversos num mesmo modo de interpretação, com o que discordamos.

Assim, se faz mister uma nova classificação, porquanto os delitos em que o alvo é o sistema informático somente de modo indireto não exigem novas formas de raciocínio, novos Princípios e novos paradigmas, exceto quanto à medição do prejuízo advindo da perda de dados. A destruição do suporte de dados é mero crime de dano.

Para o estudo em questão, tais formas de cometimento são irrelevantes porque a lesão se dá a bem jurídico já protegido, qual seja o patrimônio em sua conceituação clássica (destruir um *palmtop* atirando-o contra a parede não demandaria estudo especial do direito penal).

Quer-se focar os delitos nos quais o cometimento se faz com uso da informática (e da telemática, logicamente) violando bens jurídicos informáticos e, portanto, pressupõem-se novas premissas e novos entendimentos da realidade social.

Pela classificação de Senise, destruir um disco rígido com um martelo seria crime informático por atingir bem informacional. Contudo, não se considera tal como um delito informático puro, mas sim um delito comum em que se acaba por atingir indiretamente o sistema informático e seus dados.

Dentro da ideia de crimes cometidos contra sistemas informáticos e/ou dados (crimes informáticos próprios), há aqueles que se pode chamar de impuros (ou indiretos), como é o caso do exemplo da destruição de um *notebook* com um machado, e que implica consequentemente na destruição daquilo denominado de bens intangíveis virtuais, por ser seu suporte necessário; e há, também, os delitos que se denominará de puros (ou diretos), apresentados no terceiro exemplo, em que não há outra forma de violar os bens intangíveis senão pelo uso de meios informáticos⁸⁸.

Tal classificação nos é importante considerando-se que para os denominados delitos informáticos impuros não há qualquer exigência de método ou qualificação para o delinquente, enquanto que para o delito informático puro, pressupõe-se certo perfil, certa habilidade, certo conhecimento e certa perícia, afora as próprias particularidades do cometimento do tipo.

Não se pode olvidar que esta classificação traz uma importante preocupação com o intuito do agente. Verifica-se que ao se tratar de atos dirigidos contra o sistema informático, preocuparam-se os autores, certamente, por conhecer o perfil social dos agentes de certas condutas⁸⁹ em prever na primeira parte da definição o elemento volitivo do agente.

⁸⁸ É de Augusto Eduardo de Souza Rossini a proposta de denominação dos delitos informáticos próprios em que o alvo e o meio são informáticos como puros. Contudo, o autor aponta em sua classificação a ideia de que o ataque a bens jurídicos não informáticos em que meios informáticos são ferramentas foram denominados simples. ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos in *Direito e Internet* (coord. Edgard Moreira da Silva et al.). Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, nº 4, São Paulo, IMESP, 2002, pp. 140-141.

Nossa proposta é a sub-classificação dos delitos chamados próprios por Ivete Senise Ferreira em puros e impuros de acordo com o bem jurídico atingido diretamente.

⁸⁹ Intrusão ou invasão informática meramente como desafio (crimes de desafio), como no famoso caso de Kevin

Esta classificação referida traz, assim, mostra da preocupação dos pensadores em entender o perfil do praticante da conduta,

De acordo com Roberto Chacon de Albuquerque⁹⁰, há ainda uma classificação dos crimes informáticos que melhor representaria a proposta acima explanada, afastando interpretações equivocadas e incorretas. Seria a divisão em (i) crimes informáticos comuns e (ii) crimes informáticos específicos.

A partir de sua proposta, crimes informáticos específicos seriam aqueles em que o sistema tecnológico é o alvo da conduta – seriam os crimes que ainda carecem de legislação penal específica no Brasil, tendo-se em vista que os bens jurídicos ainda não gozam de proteção jurídica. Crimes informáticos comuns, por sua vez, são aqueles em que a informática é meio de violação de bens jurídicos já protegidos pela lei penal vigente.

A classificação aqui apresentada dá uma segunda forma para a interpretação da criminalidade em voga, uma vez que os crimes informáticos tanto específicos quanto comuns poderiam ser cometidos pelo meio informático e é trazida à baila um aspecto que muito nos interessa para a evolução do tema proposto e que será tratado adiante: o bem jurídico protegido.

Pode-se fazer uma interessante comparação da classificação em crimes comuns e específicos com uma figura do Direito Civil. Pode-se certamente considerar que a Internet é considerada como objeto de consumo ou como meio de consumo⁹¹. No primeiro caso adquire-se um serviço da própria rede (p. ex. hospedagem de *site*, provedor de acesso com conteúdo especial, etc.), enquanto que no segundo caso, a rede é meio para a aquisição de um produto em uma loja (p. ex. uso de portal de leilões ou *sites* de lojas para adquirir bens comuns, como um livro). Da mesma forma, seria o crime informático específico aquele em que é o sistema *per se* o alvo e o comum aquele em que a informática tem apenas o papel intermediário e

Mitnik que obteve a memória de operações e o número de mais de 20 mil cartões de crédito, acessou o terminal de defesa aérea norte americano, invadiu o Centro de Supercomputadores de San Diego mas demonstrou jamais ter obtido vantagem econômica com tais ações. Em 1995 foi preso e condenado a cinco anos de prisão e hoje é proprietário de uma empresa de consultoria em segurança (<http://www.kevinmitnick.com/> Acesso em 31.01.08 às 17:56hs). Fonte: http://veja.abril.com.br/entrevistas/kevin_mitnick.shtml. Acesso em 31.01.08 às 17:57hs.

⁹⁰ ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*, Editora Juarez de Oliveira, 2006, p. 40

⁹¹ Marco Antônio Zanellato, *Condutas Ilícitas na Sociedade Digital*, Caderno Jurídico – julho/02 – Ano 2- nº 4, ESMP, p.176.

eleito.

Há ainda que se apresentar uma classificação bastante útil para o estudo das dificuldades da criminalidade eletrônica, qual seja a de bens tangíveis e bens intangíveis⁹².

Uma vez que a legislação penal pátria foi, em sua maioria, constituída a partir de uma sociedade da primeira metade do século XX, priorizou-se a constituição de tipos relacionados a bens tangíveis, ou seja, a propriedade material constituída de coisas móveis e imóveis.

Bens tangíveis são aqueles que podem ser tocados e, portanto, seriam aqueles que podem pertencer a alguém, exclusivamente e de modo palpável. Bens intangíveis, por sua vez são aqueles que não podem ser tocados por só existirem imaterialmente, no mundo das ideias ou numa linguagem⁹³.

Mas não descuidou o legislador de certos aspectos econômico-sociais de difícil enquadramento da classificação da tangibilidade, pois acresceu o §3º ao artigo 155 do Código Penal, equiparando a energia elétrica (ou qualquer outra que tenha valor econômico) com o conceito de coisa móvel.

Ocorreu que do avanço científico, dos desenvolvimentos tecnológicos e da evolução dos conceitos de direito intelectual, surgiram proteções às criações autorais, às patentes e invenções, a segredos profissionais, etc. O surgimento de uma relevância econômica para bens imateriais fez com que houvesse uma modificação de paradigmas penais de proteção exclusivamente material (concepção de coisa móvel).

Se por um lado a modernização traz vantagens aparentes para a maximização de valores, por outro, reflexivamente, há o fenômeno de um descontrole da harmonia social e a criação de novos riscos, visto que, como explica Alamiro Velludo Salvador Neto:

“Assim, o legislador tipifica criminalmente as mais diversas e pensáveis condutas como apelo à voz de cidadãos inseguros. O

⁹² Também denominados corpóreos e incorpóreos, palpáveis e impalpáveis, tocáveis e intocáveis.

De acordo com Maria Helena Diniz, a classificação compreende os bens em relação a si mesmos, sendo que os bens corpóreos seriam objetos do direito e bens incorpóreos seriam aqueles que se relacionam com direitos tidos por pessoas físicas ou jurídicas sobre coisas, produtos de intelecto ou contra outra pessoa.

⁹³ O Direito Civil já considera como bem móvel incorpóreo ou intangível: (a) a propriedade imaterial, de acordo

aplicador utiliza-se irrefutavelmente deste mesmo e incessante apelo para subsumir aqueles tipos de modo severo sem qualquer comprometimento com os âmbitos de proteção estabelecidos através dos instrumentos coerentes da dogmática penal. E o jurista, por sua vez, corre desesperadamente atrás de um entendimento possível da calamitosa situação, na busca da construção de um sistema razoável para o Direito Penal da modernidade. Eis aí o fenômeno da sociedade de risco.⁹⁴”

Por conta da ciência surgiu a informática e suas peculiaridades imateriais que levaram à reclamação popular de proteção por sua importância. Conceitos como soberania, território, tempo e espaço perdem sentido e surge um novo valor vindo com a tecnologia. Novos riscos clamam por proteção penal e passa-se a concluir pela existência de um novo bem jurídico, permanente, a ser denominado “Segurança Informática”, e que merece melhor estudo.

OS TRÊS ELEMENTOS DA SEGURANÇA INFORMÁTICA

Para que o estudo da criminalidade informática pura seja bem compreendido, é necessário capacidade de entender quais os possíveis alvos de uma conduta tendo-se em vista as vulnerabilidades dos aparatos comumente atingidas.

Certamente por estar-se diante de uma sociedade de risco “*sui generis*” necessário se faz entender que tal conceito está diretamente relacionado com a falta de segurança frente à ideia de liberdade⁹⁵. Por segurança, compreende-se a condição de algo ou alguém encontrar-se livre de perigo, perdas ou proteção.

Assim, é possível que se limite, com base na análise empírica dos crimes mais

com o art. 5º da Lei 9.279/96; e (b) os direitos autorais, de acordo com o art. 3º da Lei 9.610/98.

⁹⁴ SALVADOR NETO, Alamiro Velludo. **Tipicidade Penal e Sociedade de Risco**. Quartier Latin, São Paulo, 2006, p.85. No mesmo sentido, BERG, Sara E., Op. cit., p. 228.

⁹⁵ Nas palavras de Ricardo M. Mata y Martín *apud* ROSSINI, op. cit, p. 132: “(...) a expressão da liberdade do indivíduo e consiste no direito a utilizar lícita e livremente, com os limites constitucionais e legais, a tecnologia informática. De forma que os delitos informáticos podem ver-se como violação dessa mesma liberdade informática, como infração de distintas liberdades as que podem estender-se ao emprego destas tecnologias (intimidade, domicílio, livre circulação, associação etc.)”.

corriqueiros que envolvem tecnologia, os componentes que tornam um sistema de informática inseguro, por serem três os pilares que sustentam o conceito de ambiente informático.

São os três elementos, de acordo com o Preâmbulo da Convenção de Budapeste sobre Cibercrime e também de acordo com o Comitê Gestor da Internet no Brasil, a confidencialidade, a integridade e a disponibilidade⁹⁶. A ver:

*“Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a **confidencialidade, integridade e disponibilidade de sistemas informáticos**, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;”* (grifo nosso)

Partindo destes como os pressupostos da segurança, natural e respectivamente encontram-se três valores na sociedade de informação que tomarão vulto para proteção jurídica.

CONFIDENCIALIDADE

A confidencialidade é a garantia de sigilo no que se refere às informações tratadas pelos aparatos informáticos e que pertencem a um número individualizável de usuarios, não sendo, pois, pública e não podendo ser lida, utilizada ou de qualquer modo acessada por

⁹⁶ Convenção sobre o Cibercrime. Budapeste, 23.XI.2001. Disponível em http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf. Acesso em 01.01.08 às 13:16hs.

Conforme DIJK e KELTJENS, seriam os três elementos a (i) disponibilidade de meios, (ii) a integridade de sistemas e dados, e (iii) a exclusividade de meios e dados. DIJK, Chr. H. van e KELTJENS, J.M.J.

qualquer pessoa que não seja legítima ou legitimada. Isso se dá porque é de se compreender o material informático como verdadeira propriedade de um indivíduo. E conforme Bobbio⁹⁷

“o substantivo propriedade deriva do adjetivo latino proprius e significa ‘que é de um indivíduo específico ou de um objeto específico (nesse caso, equivale a: típico daquele objeto, a ele pertencente), sendo apenas seu’. A etimologia oferece os traços de uma oposição entre um indivíduo ou um objeto específico e o resto de um universo de indivíduos e de objetos, como categorias que se excluem reciprocamente”.

Conclui-se que tal valor aponta para o caráter particular dos dados produzidos ou guardados pelos aparatos informáticos, seguidos da restrita permissão para terceiros acessarem conteúdos, limitada a autorização do real proprietário. Desta maneira, é de se concluir que dados existentes dentro de um aparato celular como a agenda telefônica ou o arquivo de mensagens enviadas, pertencem exclusivamente ao legítimo detentor, ao produtor dos dados, ou àqueles que receberam acesso autorizado pelo mesmo, a tal conteúdo.

Do mesmo modo, o acesso a uma senha ou a um filme existentes dentro de um computador só pode ocorrer pelo rol de usuarios que compõe a lista de acesso autorizado pelo proprietário de tal ativo (no caso, bem intangível com valor), seja mediante pagamento, seja gratuitamente. A confidencialidade de uma informação está diretamente relacionada com o interesse e a vontade de um usuario-proprietário, que tem como prerrogativa poder dispor de tal ativo e decidir o quão amplo será o conhecimento e o quão livre será a inserção de tais dados.

A intrusão informática, a leitura de *e-mails* não autorizada, o acesso às informações particulares como senhas e dados bancários ou comerciais, o acesso ao correio eletrônico alheio para remetimento e difusão de *malwares* ou propaganda, a leitura ou uso de senhas pessoais, número de cartão de crédito, e até o assistir de filmes e o ouvir de músicas sem autorização dos produtores, são alguns exemplos de condutas que violam diretamente a

Computercriminaliteit. Zwolle. W.E.J., Tjeenk Willink, 1995, p. 6 *apud* ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática. Editora Juarez de Oliveira, São Paulo, 2006, p. 47.

confidencialidade a dados.

A reprodução de tais dados de modo a dar acesso a outrem e a divulgação, gratuita ou onerosa, mostram-se igualmente violadoras de tal condição, caso os legítimos proprietários ou disponibilizadores não tenham anuído com tais publicidades, amplas ou restritas.

É a confidencialidade, em suma, a qualidade de um dado manter-se restrito a acessos alheios até que haja permissão para tanto, dada por alguém legitimado.

INTEGRIDADE

O conceito de integridade é deveras equívoco, vez que passa uma primeira impressão de materialidade. Íntegro poderia ser erroneamente conceituado como algo que está fisicamente mantido completo em sua origem. Um papiro pode ser encontrado íntegro em escavações, um refém pode ser resgatado íntegro de um cativo.

Contudo, dados e sistemas não são físicos ou tangíveis nem são compreensíveis num mundo material, necessitando de um aparato que os traduza, torne equivalentes e os traduzam. Também, não podem sequer serem conceituados como coisas por faltar-lhes equiparação legislativa.

O melhor e mais compreensível sinônimo para integridade seria inteireza. É ínsito ao Direito Penal informático, quando se pensa em dados e em sistema, a ideia de fracionabilidade e divisibilidade.

Todo o qualquer dado com valor econômico (ativo), seja um documento escrito em editor de texto, seja uma foto ou arquivo de áudio, existe porquanto foi escrito em uma linguagem especial. Esta chamada linguagem de programação nada mais é do que uma sequência de linhas escritas e que são decodificadas pela máquina que a exibe de maneira que seres humanos consigam entender.

Ocorre, entretanto, que as máquinas informáticas somente são capazes de entender uma

⁹⁷ BOBBIO, Norberto *et al.*, Dicionário de Política. 7a. edição. UnB. Brasília. 1995, v. 2, p.1.021.

linguagem composta de zeros (0) e uns (1) que, respectivamente, correspondem a ausência ou a existência de estímulos elétricos⁹⁸. A composição de um arquivo elaborado por um usuário é feita de maneira perfeita, precisa e automática. Os programas, com a ajuda do maquinário, formam as linhas de programação de maneira a tornarem os dados exatos, codificados para armazenamento e decodificáveis para uso. A integridade, assim, para o desenvolver de nosso trabalho, será compreendida como a incolumidade de dados ou informações na origem, no trânsito ou no destino, de acordo com o Decreto no. 4.553 de 30.12.2002⁹⁹.

É prerrogativa do usuário que seus dados existam na forma como foram criados, copiados ou armazenados, sendo vedada sua modificação por terceiros sem autorização, especialmente tendo-se em vista tratar-se de propriedade com valor econômico. Uma alteração em um arquivo pode torná-lo imprestável, gerando prejuízos patrimoniais de grande ordem.

É, também, imprescindível que, caso seja autorizada qualquer modificação (por exemplo a atualização do arquivo referente ao banco de dados dos vírus existentes para busca e combate pelo *software* antivírus), tal modificação seja clara e transparente quanto aos impactos que trará à funcionalidade do sistema, programa ou arquivo, além de autorizada expressamente pelo usuário.

De tal sorte, a modificação de dados originais – de sua programação, portanto – pode levar a uma deturpação de seu fim, impedindo-o de servir para os fins aos quais foram criados.

⁹⁸ Cada impulso elétrico composto da linguagem binária (0 ou 1) denomina-se BInary DiGiT, ou simplesmente *BIT*. Uma vez que a informática processa automaticamente um número larguíssimo de dígitos binários para ser capaz de retratar um som ou uma animação, criou-se uma padronagem. Oito *bits*, ou oito sinais binários, formam um byte. A partir dos bytes, grupamentos de 1024 unidades⁹⁸ passam a ter novas nomenclaturas (1024 bytes formam um Kbyte; 1024 Kbytes formam um Mbyte; 1024 Mbytes formam um Gbyte e assim por diante). Com base em uma tabela denominada **ASCII** (*American Standard Code for Information Interchange* ou Código Padrão Americano para o Intercâmbio de Informação), cada byte (desde 0000 0000 até 0111 1110) representa um comando, símbolo, número ou letra, levando-se, pois, à compreensão humana a decodificação do sinal binário. Tal raciocínio serve-nos para demonstrar o quanto longo em termos de sinais binários pode ser uma palavra como “BOLA”, pois que composta de quatro letras e, portanto, ao menos 4 sequências de 8 *bits*, ou 4 bytes. A partir disso podemos, pois, compreender o quanto importante para a decodificação da palavra BOLA de binário para nossa linguagem é a ordem correta que devem estar dispostas as linhas de programação. Um simples erro na codificação ou na decodificação pode inutilizar todo o arquivo.

⁹⁹ O Decreto nº 4.553 de 27 de dezembro de 2002 “dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências”. Em seu artigo 4º. Inciso VIII, o conceito de integridade surge como “VIII- integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;”

A modificação de um simples *bit* de uma programação pode fazer com que um arquivo seja corrompido e não mais possa ser lido pelos aparatos, ou pode fazer com que tal arquivo acabe por cumprir uma função para a qual não estava programado. A mudança do estado inteiro de um arquivo pode torná-lo totalmente inadequado para seu uso original e até mesmo implicar em sua destruição.

São exemplos de condutas em que se visa violar a integridade de um arquivo – que pode existir por si ou pode fazer parte de um sistema – o cibervandalismo, a inserção de *malware* para destruição de arquivos, a modificação de linhas de programação para inutilizar arquivos, a quebra de senhas, a inserção de arquivos (*cracks*) que permitem o uso de *softwares* piratas ludibriando os sistemas de verificação de autenticidade, dentre outras, pois que de alguma forma modificam arquivos e fazem com que seu uso ou seja modificado, ou impedido.

DISPONIBILIDADE

A tecnologia desenvolvida pelo homem visa à melhoria e facilitação das tarefas diuturnas. Por isso, foi trazida ao dia-a-dia para servir ao homem, no momento em que este precisa ou deseja utilizá-la.

Os aparatos informáticos têm como característica a sua disponibilidade, permitindo que seus proprietários possam utilizar-se deles para a tradução dos dados e cumprirem seus objetivos através da execução de comandos.

Não basta que os dados e seu conteúdo estejam resguardados do acesso não autorizado de terceiros e nem que estejam íntegros, em perfeito estado de inteireza, se seu legítimo proprietário não consegue ter acesso a eles ou permitir que terceiros o tenham. É necessário que para consolidar o conceito de segurança informática tenha-se a ideia de acessibilidade ampla para o usuário autorizado.

Compõe a segurança da informação a possibilidade livre de o usuário utilizar-se de seus dados no momento em que desejar. Tal acesso deve ser livre de embaraços e incômodos, sem intervenções e em condições razoáveis. O citado Decreto nº. 4.553/2002 conceituou disponibilidade como sendo a facilidade de recuperação ou acessibilidade de dados e

informações¹⁰⁰.

A percepção deste valor como ínsito à segurança telemática se deu por conta de que diversos *malwares* e certas técnicas, ao invés de destruir dados, acabam por levar a uma sobrecarga do sistema informático, tornando-o lento e por vezes até inacessível, sem que os dados contidos em si jamais cheguem a ser lidos por qualquer usuário desautorizado ou prejudicados, até por faltar-lhe dolo de violar tais aspectos da segurança telemática. O mesmo pode ser argumentado quanto à arquivos modificados por delinquentes a ponto de impedirem que seus legítimos detentores possam ter acesso.

Percebendo-se que a indisponibilidade dos dados poderia ser tão prejudicial quanto à destruição dos mesmos e até quanto à sua confidencialidade, inegável é que a disponibilidade compõe fundamentalmente a essência da informática como terceira perna de sustentação.

Analogicamente, de nada adianta ter-se um cofre com um segredo guardado dentro, íntegro, se não se conhece a senha para abrir a tranca e a porta.

As condutas mais comuns, violadoras da disponibilidade são os ataques a provedores denominados DoS (*Denial of Service*), o erroneamente chamado “sequestro” de arquivos¹⁰¹, a inserção de *malware* seguida de acesso e modificação da senha de *email* ou rede social alheia, a inserção de *malwares* que se multiplicam tornando o uso da máquina lento, o envio de arquivo que se instala na máquina alheia e a reinicializa constantemente, entre tantas outras.

UM NOVO BEM JURÍDICO

A ideia de bem jurídico está ligada a valores que devem ser protegidos pelo Direito Penal, especialmente pelo fato de que o Estado democrático de Direito deve garantir a seus cidadãos o desenvolvimento pacífico e a coexistência de semelhantes em igualdade de

¹⁰⁰ Decreto nº 4.553 de 27 de dezembro de 2002, artigo 4º, inciso VI.

¹⁰¹ O artigo 159 do Código Penal é explícito ao apontar que o termo “sequestro” somente é utilizado nesta ciência no sentido de privação de liberdade de uma pessoa, não sendo cabível qualquer extensão interpretativa – mesmo porque “*in malam partem*” –, muito especialmente ao se tratar de objetos intangíveis como dados informáticos. A privação da disponibilidade de arquivos com a consequente tentativa de obter vantagens patrimoniais configura crime de extorsão previsto no artigo 158 do mesmo *Códex* pois que a promessa de mal injusto (destruição de arquivo ou indisponibilidade) está configurada.

condições necessárias, verdadeiramente como mantenedor da ordem social¹⁰².

Por isso, os objetos que devem ser garantidos para que tais objetivos sejam atingidos justificam o contrato social e têm sua existência mantida pela força central coativa¹⁰³. Por tal motivo, Francisco Assis de Toledo aponta que:

*“A soma dos bens jurídicos constitui a própria ordem social, e por isso, o significado de um bem jurídico não deve ser apreciado isoladamente, mas sim, em conexão com toda a ordem social”*¹⁰⁴

Afora o questionamento acerca da necessidade de os Estados interferirem na nova sociedade da informação, mais especialmente em seu ambiente virtual, boa parte dos governos da Europa e Américas¹⁰⁵ já decidiram por elaborar normativos tendentes a impor limites à Internet, à troca de informações por meio da tecnologia, e a própria sociedade já compreendeu que os dados são ativos intangíveis e que a cada dia estamos mais propensos a depender da informática.

¹⁰² O bem jurídico, segundo Miguel Polaino Navarrete, seria o bem ou o valor merecedor da máxima proteção jurídica, cuja outorga é reservada às prescrições do Direito Penal. *Apud* CÂMARA, Guilherme Costa. Programa de Política Criminal Orientado para a Vítima de Crime. Co-Edição Coimbra Editora e Editora Revista dos Tribunais, São Paulo, 2008, p. 52.

¹⁰³ ROXIN, Claus. A proteção de bens jurídicos como função do Direito Penal. (Organização e tradução de CALLEGARI, André Luiz e GIACOMOLLI, Nereu José. Livraria do Advogado Editora, Porto Alegre, 2006, pp. 16-20

¹⁰⁴ TOLEDO, Francisco de Assis. Principios Básicos de Direito Penal. 5ª Edição. Editora Saraiva, São Paulo, 2002, p. 15-16.

¹⁰⁵ Na Europa, a “Convention on Cybercrime (Treatie n. 185)” teve como signatários Albânia, Armênia, Áustria, Azerbaijão, Bélgica, Bósnia-Hezegovina, Bulgária, Croácia, Chipre, República Tcheca, Dinamarca, Estônia, Finlândia, França, Geórgia, Alemanha, Grécia, Hungria, Irlanda, Groelândia, Itália, Letônia, Lituânia, Lichtenstein, Malta, Moldova, Montenegro, Holanda, Noruega, Polônia, Portugal, Romênia, Sérvia, Eslováquia, Eslovênia, Espanha, Suécia, Suíça, Macedônia, Ucrânia e Grã-Bretanha. Não membros do conselho da Europa que também assinaram a convenção: Canadá, Japão, África do Sul e Estados Unidos da América do Norte. Dados disponíveis no site do Conselho da Europa em <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=1/4/2009&CL=ENG>. Acesso em 04.01.09 às 12:33hs.

De acordo com Roberto Chacon de Albuquerque, também a Nova Zelândia já adotou leis específicas para delitos informáticos. ALBUQUERQUE, Roberto Chacon de. Op. cit., p. 31.

Na América, a Venezuela possui Lei Especial contra os delitos informáticos, conforme ROSSINI, Augusto. Op. cit., pp. 341-352.

A Argentina, afora sua legislação contra SPAM (Ley de Proteccion de los Datos Personales) em 24 de junho de 2008, aprovou a Lei 26.388 que modificou o Código Penal, adequando-o para a punição de delitos informáticos. <http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm>. Acesso em 04.01.09 às 12:49hs.

Também Chile, México e Peru apresentam normativos tipificadores de delitos informáticos. LIMA, Paulo Marco Ferreira. Op. cit. pp. 97-98.

A justificativa para a ideia de ser a rede um bem jurídico pode ser observada no seguinte excerto de Claus Roxin:

“Um conceito de bem jurídico (...) não pode ser limitado, de nenhum modo, a bens jurídicos individuais; ele abrange também bens jurídicos da generalidade. Entretanto, estes somente são legítimos quando servem definitivamente ao cidadão do Estado em particular. (...) Ele se diferencia do assim denominado conceito metódico de bem jurídico, segundo o qual como bem jurídico unicamente se deve entender o fim das normas, a ratio legis”¹⁰⁶.

A Internet e as tecnologias terminam por mostrarem-se exatamente deste modo: servem a cada cidadão em particular, mas são gerais por representarem avanço de toda uma coletividade.

Tendo em vista tais premissas e os sustentáculos formados pelos valores integralidade, confidencialidade e disponibilidade que a segurança informática deve ser considerada um novo bem jurídico a ser protegido e suas três vertentes.

A informática e seus deslindes afetam de maneira uniforme toda a sociedade global, uma vez que a tecnologia mostra-se imprescindível para o evoluir humano. Exceção feita a segmentos cada dia mais diminutos em que a informática não atinge, todos estamos permeados pelos conceitos da tecnologia que apresenta suas vantagens inquestionáveis. Direta ou indiretamente, todos estão vinculados às máquinas e a violação deste segmento cria dificuldade sobremaneira ao desenvolvimento.

Da mesma forma, mesmo que não se esteja próximo a rios e florestas, sua preservação é fulcral para o ser humano; por mais que não se tenha filhos, a infância e adolescência, com sua fragilidade, devem ser resguardada. A sociedade da informação e sua segurança informática clama pela mesma cautela.

Gianpaolo Poggio Smanio defende que três são as categorias de bens jurídico-penais, a saber: 1) os de natureza individual – disponíveis, sem afetação de terceiros; 2) os de natureza

¹⁰⁶ ROXIN, Klaus. Op. cit. p.19-20.

coletiva – indisponíveis, pois que afetam terceiros pertencentes a um mesmo grupo; e 3) os de natureza difusa – também indisponíveis, mas que afetam todos os grupos de indivíduos¹⁰⁷.

A nova sociedade da informação surgida com a Revolução Digital – e a Internet, as comunicações por satélite e tecnologias como, por exemplo *bluetooth* – fez surgir um verdadeiro meio ambiente informático.

A informática e a rede mundial de computadores trouxeram vantagens a ponto de fazer com que uma grande quantidade de pessoas aderisse ao conceito de vida virtual e até mesmo dependência virtual¹⁰⁸. As transformações da informática, recentemente, voltaram-se para a criação de produtos que levassem ao usuário a ideia de que se poderá (*rectius*, pode) encontrar na virtualidade as ferramentas para todas as tarefas que cada um precisa exercer, sem que com isso haja um aumento de custos.

O uso de recursos *on-line*, fez surgir, assim os conceitos “*cloud computing*” e “*SaaS - Software-as-a-Service*”, traduzido para o vernáculo como “computação nas nuvens” ou “Programas como serviços”.¹⁰⁹

A rede em seu conceito mais moderno, substituiu uma grande quantidade de tarefas da vida de cerca de um quinto da população¹¹⁰, sendo possível, através dos serviços oferecidos, fazer compras, manter relacionamentos, ter lazer, fazer reuniões de negócio, pagar contas entre tantas outras tarefas¹¹¹.

¹⁰⁷ SMANIO, Gianpaolo Poggio. Tutela Penal dos Direitos Difusos. Atlas, São Paulo, 2000, p. 108.

¹⁰⁸ Em artigo sobre a etiologia da dependência informática, em especial a dependência sexual, Michael Pittaro apresenta que há uma verdadeira “Desordem por Dependência da Internet” (Internet Addiction Disorder) semelhante a da dependência (vício) por jogos de azar chegando mesmo a ser uma forma de transtorno obsessivo compulsivo em alguns casos. PITTARO, Michael. Sexual Adiction to the Internet: from curiosity to compulsive behavior. In Crimes of the Internet (editado por Frank Schmallegger), Pearson Prentice Hall, New Jersey, 2008, pp. 5-6.

¹⁰⁹ A expressão advém de pesquisas e informes provenientes da empresa Google Inc. que desenvolve serviços on-line e gratuitos, que dispensam o uso de computadores demasiadamente avançados e poderosos, levando a inserção cada vez maior de pequenas empresas e fornecedores de serviços. Tal tendência levaria a um barateamento da informática e maior sedução para acesso constante (e, pois, maior dependência), simplificando a tarefa dos computadores a de uma plataforma de acesso às aplicações, que estariam disponíveis em uma grande nuvem denominada Internet.

Nesse sentido, matéria publicada na revista INFO de Dezembro de 2008, Editora Abril, intitulada “Você está nas nuvens”, pp. 69-81.

¹¹⁰ Cerca de 21,2% da população mundial tem acesso à Internet segundo <http://www.Internetworldstats.com/stats.htm>. Acesso em 13.06.08 às 18:21hs.

¹¹¹ Levando-se em conta apenas a Internet, o brasileiro passa uma média mensal de 23 horas e 50 minutos

Isso se dá porque a rede com sua plataforma crescentemente amigável tende a tomar conta de nosso cotidiano. Nota-se, inclusive, que plataformas já foram criadas para fazer com que o usuário simule uma segunda vida dentro da rede e cada vez mais dependa dela, crie uma identidade e conte com comodismos¹¹².

A envergadura que tomou a rede fez com que houvesse uma forte migração das estratégias comerciais e eleitorais para a Internet, levando o usuário a uma sobrecarga de mensagens não solicitadas.

Também, o desenvolvimento de *cookies* faz com que se elevem as estratégias invasivas (algumas delas conhecidas como KYC ou “*know your customer*” ou “conheça seu consumidor”, em tradução livre) em que a navegação em *sites* de compra faz com que sejam instalados pequenos programas que memorizam as preferências do cliente conforme ele navega pelas páginas e informam o fornecedor, para que ele melhor direcione suas ofertas.

Indubitavelmente a Internet tornou-se um novo veículo de comunicação em massa. Assim como a televisão ou o rádio, há programações e há comerciais e levou um tempo até que se popularizasse. Hoje, já popular e em vertiginoso crescimento, é mais do que um meio de relacionamento e uma ferramenta: tornou-se parte da cultura do ser humano.

O estudo do Direito Ambiental leva-nos a concluir que dois são os tipos de meio ambientes: os naturais e os artificiais. Os meio ambientes naturais ou físicos foram definidos pelo artigo 3º. Da Lei 6.938/81 e devem ser compreendidos como sendo:

“Art 3º - Para os fins previstos nesta Lei, entende-se por:

I - meio ambiente, o conjunto de condições, leis, influências e interações de ordem física, química e biológica, que permite, abriga e rege a vida em todas as suas formas;

conectado. Considerando-se que apenas dois terços do dia permanecemos acordados, conclui-se que, num mês de trinta dias, ficamos cerca de 5% do tempo navegando pela rede e tais estatísticas não levam em conta, por exemplo, pessoas que trabalham o tempo inteiro conectados, sem dedicação à navegação. <http://tecnologia.terra.com.br/interna/0,,OI3139143-EI4802,00-Brasil+internautas+batem+recorde+em+numero+e+tempo+de+navegacao.html>. Acesso em 03.02.09 às 18:25hs.

¹¹² Exemplos são programas simuladores de ambiente tridimensional como o “*Second Life*” e “*Google Lively*” em que o usuário simula tarefas do dia a dia a partir da criação de um *avatar*, ou seja, uma personagem virtual com as características desejadas pelo usuário, para que ele promova execução de tarefas corriqueiras como ir ao banco, visitar uma loja, etc. Sites: www.secondlife.com e www.lively.com, ambos com acesso em 01.01.09 às 18:02hs.

II - degradação da qualidade ambiental, a alteração adversa das características do meio ambiente;

III - poluição, a degradação da qualidade ambiental resultante de atividades que direta ou indiretamente:

a) prejudiquem a saúde, a segurança e o bem-estar da população;

b) criem condições adversas às atividades sociais e econômicas;

c) afetem desfavoravelmente a biota;

d) afetem as condições estéticas ou sanitárias do meio ambiente;

e) lancem matérias ou energia em desacordo com os padrões ambientais estabelecidos;

IV - poluidor, a pessoa física ou jurídica, de direito público ou privado, responsável, direta ou indiretamente, por atividade causadora de degradação ambiental;

V - recursos ambientais: a atmosfera, as águas interiores, superficiais e subterrâneas, os estuários, o mar territorial, o solo, o subsolo, os elementos da biosfera, a fauna e a flora.”

Em contrapartida ao meio ambiente natural está o meio ambiente artificial que pode ser entendido como aquele em que o homem interveio, modelando de acordo com sua vontade e necessidade a forma como seria construído e desenvolvido. Dentre os meio ambientes artificiais, pode-se enquadrar os denominados meio ambiente cultural e meio ambiente de trabalho, entre outros.

Manuel Castells, sociólogo espanhol, afirmou que a Internet é uma criação cultural¹¹³. Mas afinal, para que serve a tecnologia informática e, mais especialmente a rede mundial de computadores? A reunião de redes interligadas em escala mundial e a possibilidades de comunicação via outras tecnologias (rádio, satélites, etc) é uma plataforma de troca de informações que tem como uso precípua, por constituição, a comunicação em tempo real, a cultura, o entretenimento, a educação, o marketing e o trabalho, *inter alia*.

José Afonso da Silva, explicando meio ambiente cultural, apõe que compõe tal meio ambiente o patrimônio histórico, artístico, arqueológico, paisagístico e turístico, e explana que

¹¹³ CASTELLS, Manuel. A Galáxia da Internet – Reflexões sobre a Internet, os negócios e a sociedade. Jorge

merecem o direito constitucional de preservação¹¹⁴, de acordo com o art. 30, inciso IV, da Carta Magna. É tal meio ambiente aquele que reflete os aspectos que compõe a cultura de uma população em seu aspecto mais amplo.

Sociologicamente, o vocábulo “cultura” quer significar o sistema de ideias, conhecimentos, técnicas e artefatos, de padrões de comportamento e atitudes que caracterizam uma determinada sociedade. Antropologicamente, é o estágio do desenvolvimento cultural de um povo, caracterizado pelo conjunto das obras, instalações e objetos criados pelo homem desse povo¹¹⁵.

A nosso ver, meio ambiente artificial pode ser entendido como aquele meio ambiente em que o ser humano, social por natureza, vive também. Como estamos em constante evolução, sofre o meio ambiente as alterações necessárias para satisfazer aquilo para o que o destinamos.

Ainda que não se possa enquadrar perfeitamente o conceito de meio ambiente à rede mundial de computadores e à rede informática como um todo por conta da expressão “ordem física”, é assim que deve ser vista a tecnologia que tomou parte na vida hodierna: como um verdadeiro meio ambiente construído, e que faz parte da cultura do homem.¹¹⁶

Importante que se note que a quantidade de postos de trabalho focados na criação de informações na forma de dados cresce a cada ano, além do fato do que a grande maioria dos postos de trabalho oferecidos, hoje, exigem que o candidato tenha conhecimento em informática. Isso se dá pelo fato de que a informática e as noções de Internet, cada dia mais se mostram componentes do próprio meio ambiente de trabalho.

Por meio ambiente do trabalho (previsto no artigo 200, VIII da Constituição Federal¹¹⁷) entende-se, brevemente por não ser objeto deste trabalho, o conjunto de fatores naturais e características artificiais que compõem o local de trabalho de uma pessoa.

Zahar Editor, Rio de Janeiro, 2001, pp. 34-55.

¹¹⁴ SILVA, José Afonso da. **Direito ambiental constitucional**. 5a. edição. Malheiros, São Paulo, 2004, p. 20-21.

¹¹⁵ Dicionário Eletrônico Michelis. <http://michaelis.uol.com.br/moderno/portugues/index.php?palavra=cultura>. Acesso em 01.01.09 às 18:18hs.

¹¹⁶ “A Internet é o tecido de nossas vidas” - CASTELLS, Manuel . “A Galáxia...” Op. cit. p. 7.

¹¹⁷ Art. 200. Ao sistema único de saúde compete, além de outras atribuições, nos termos da lei: (...) VIII - colaborar na proteção do meio ambiente, nele compreendido o do trabalho.

Por certo houve modificações na organização do trabalho por conta de novas tecnologias que exigem um novo estilo de trabalhador, com habilidades de abstração, comunicação e integração¹¹⁸.

Assim, minimamente como acessório de outro meio ambiente está a estrutura informática (cultural ou do trabalho) e, pois, trata-se de bem jurídico-penal difuso, cabendo, inclusive, a proteção fulcrada na Lei nº 7.347/85 (Lei da Ação Civil Pública).

Se conseguir-se o entendimento de que a existência de recursos tecnológicos adequados compõe o meio ambiente artificial, pode-se açambarcar em tal conceito as ideias de que meios ambientes sofrem alterações e podem tornar-se adequados ou inadequados para o fim a que se destinaram. Para tanto, precisa-se pressupor que um espaço virtual traz ínsito em si condições que o tornam impróprio e que devem ser combatidas.

Ainda que o ambiente seja totalmente virtual, a tecnologia tornou possível que a navegação através da rede fosse visualizada, pois que traduzida em recursos multimídia. Assim, o ingresso em um *site* é visível e mostra-se na tela com logotipos, coloridos peculiares, formatação de tela, sons, vídeos, ofertas publicitárias, entre tantas características. É a partir desses componentes que se pode incluir no ambiente virtual conteúdos culturais, laborais, artísticos, dentre tantos outros.

Ocorre que a crescente dependência humana pela tecnologia, leva a uma consequente dependência por um ambiente virtual viável, para que a vida possa manter-se em normal andamento. Assim como é necessário que ar, água e florestas estejam protegidos para que condições mínimas sejam mantidas, o mesmo se pode pensar quanto ao ambiente virtual.

O ser humano que, em seu ambiente físico de trabalho, exige proteções – auriculares, oculares, em relação a excesso ou diminuição de temperatura, e até mesmo quanto a assédios morais – acaba por ficar totalmente desprotegido no que tange ao ambiente de trabalho (quicá

¹¹⁸ Essas habilidades são próprias de serem aprendidas na escola durante a instrução regular, e esta é a raiz do recente interesse das classes dominantes pela qualidade escolar, ao contrário do período anterior ao esgotamento do padrão taylorista-fordista, no qual a educação desempenhava um papel periférico, pois o trabalhador não precisava de grandes conhecimentos técnicos ou de habilidades especiais, sendo preparado na própria linha de produção através do treinamento. www.unisc.br/cursos/enade/docs/curso_enade/Sociedade_Rede_paradigma_informacional.doc Acesso em 14.07.08 às 15:26hs)

acessório) que mais cresce: a rede mundial de computadores e a garantia de seu funcionamento razoável.

Dessa forma, a segurança informática mostra-se merecedora de proteção penal uma vez que dependendo do grau, sua afetação leva prejuízo a toda à coletividade, mostrando-se como bem jurídico-penal de natureza difusa, pois que as conexões tecnológicas e a virtualidade configuram verdadeiro meio ambiente¹¹⁹. É a virtualidade, sem dúvidas, uma nova plataforma de interação e relação social que toma mais espaço à medida em que a brutal realidade amedronta os cidadãos.

Há, também, quem chegue a considerar que a lesão dentro da rede chega a violar mesmo os direitos humanos, como é o caso de Yvonne Jewkes que apresenta:

*“A garantia de segurança pessoal é considerada como um direito humano fundamental, ainda que o escopo e a permeabilidade das tecnologias digitais abram novas áreas de vulnerabilidade social.”*¹²⁰

Mas a ideia de bem difuso não é única. Não se olvide que o raciocínio apresentado deve levar em conta a capacidade lesiva da atitude cometida na rede, pois que não há que se considerar violado um bem difuso quando do envio de uma mensagem que ofenda bem jurídico privado exclusivamente, nem bem jurídico já protegido por outra norma. Isto posto, condutas que aviltem a rede como um todo merecem o título de violadoras de bem jurídico difuso como a propagação incontrolada de *malwares* ou o ataque de negação de serviço a um provedor de conteúdo da Internet que violam razoável segurança da rede.

Ricardo M. Mata y Matin, por sua vez, aponta que uma nova dogmática penal deve ser construída, com base na segurança informática, mais especificamente denominada “liberdade informática” e apresenta que:

¹¹⁹ Vide dificuldades surgidas com os problemas técnicos experimentados pela empresa Telefônica em julho de 2008, em que evento técnico fez com que milhares de usuários restassem sem conexão, inclusive órgãos da Administração Pública do Estado de São Paulo e municípios. <http://tecnologia.uol.com.br/ultnot/2008/07/03/ult4213u474.jhtm>. Acesso em 01.08.08, às 11:13hs.

¹²⁰ “The entitlement to security of person is regarded as a fundamental human right, yet the scope and pervasiveness of digital Technologies open up new areas of social vulnerability” JEWKES, Yvonne. Dot.cons:

“(...) a expressão da liberdade do indivíduo e consistente no direito a utilizar lícita e livremente, com os limites constitucionais e legais, a tecnologia informática. De forma que os delitos informáticos podem ver-se como violação dessa mesma liberdade informática, como infração das distintas liberdades as que podem estender-se ao emprego dessas tecnologias (intimidade, domicílio, livre circulação, associação, etc)”¹²¹”

Há que se dizer que são algumas das condutas que ora classifica-se como delitos informáticos próprios (puros ou impuros) que terminam por lesar a coletividade com as características que se apresentam acima.

Contudo não são somente os crimes próprios que trazem características especiais. Certamente que há peculiaridades nos crimes informáticos impróprios – crimes comuns cometidos pela eleição do computador como meio – que por serem cometidos com o uso da informática levam a sociedade a inseguranças e fragilidades também. O uso do meio ambiente *sui generis* é fator que agrava e aumenta a perspectiva da conduta seja porque encoraja a ação de um delinquente, traz sensação de impunidade e até mesmo viola um grande número de pessoas,.

Os bens jurídicos já protegidos e que são lesados por meio do uso da tecnologia – como, por exemplo a honra atacada por uma mensagem de texto remetida por celular –, não merecerão nova roupagem, por já serem objeto de proteção. Mas as condutas praticadas merecem alternativas de agravamento, vez que praticadas por meio facilitador e com alta capacidade lesiva e, mais especialmente, por serem uma tendência da criminalidade.

Não se pode então confundir o ataque a um bem jurídico difuso com um ataque maciço (e múltiplo) a bens jurídicos individuais graças à força propulsora da informática.

A rede mundial e a tecnologia mostraram-se uma tendência irrefutável da sociedade. A evolução do novo meio socializante terá cada dia mais adeptos. Certamente, o crescimento de

crime, deviance and identity on the Internet. Willan Publishing, Devon, 2003. p. 24.

¹²¹ *apud* ROSSINI, Augusto Eduardo de Souza. In “Informática, Telemática e Direito Penal”, Memória Jurídica Editora, São Paulo, 2004, p.132

usuários levará a um consequente crescimento de ativos, ou seja, de informações com valor pecuniário direto ou indireto, seja no mercado, seja na criminalidade.

É desiderato que o novo meio faça com que boa parte dos serviços da cadeia produtiva siga-o, uma vez que a virtualidade leva a maior velocidade comercial, melhor relacionamento com o cliente, prontidão de atendimento, diminuição de custo com mão de obra e aumento de lucros pois a Internet faz com que tudo que nela está chegue a todos, sem fronteiras nem limites. É uma tendência que agrada fornecedor e consumidor e, assim, torna-se (ou tornar-se-á em breve) fulcral ao crescimento¹²².

Por tal motivo, o uso da rede mundial de computadores como meio ou o ataque a ela tendem a ser uma tática merecedora de maior pena. O envenenamento de água, o corte de energia elétrica, a destruição das comunicações, a sabotagem à produção de alimentos. Todos são alvos essenciais ao desenvolver humano, assim como é a rede mundial.

O que é apresentado é somente um novo bem que merece a proteção legislativa, vez que certas condutas não são juridicamente relevantes se levado em conta somente os valores já existentes¹²³.

É o caso da invasão de um computador através de brecha de segurança sem que o invasor promova qualquer destruição; é o caso de um usuário que se apodera do número de cartão de crédito de diversos usuários sem deles fazer uso e, ainda, é o caso da inserção de código malicioso que simplesmente torna um sistema lento. Sem o estabelecimento de um novo valor jurídico-penal lesado, permanece a ideia de que tais condutas em nada prejudicam a sociedade em qualquer segmento, sendo que, na realidade, transformam o ambiente informático – que é imprescindível pois toma mais e mais o vulto de predominante nas relações em geral –, que é difuso em certos aspectos, em um ambiente inseguro.

¹²² A rede foi denominada “*Triple A Engine*” ou mecanismo dos três “A’s” por conta de a Internet caracterizar-se por sua “*Acessibility*” (Acessibilidade), “*Anonymity*” (Anonimidade) e “*Affordability*” (“Arcabilidade” – possibilidade de se poder arcar com seus custos), conforme COOPER *et al* in *Online sexual activity: An examination of potentially problematic behaviors. Sexual Addiction & Compulsivity*. New York, 2004, pp.129-143 *apud* *Crimes of the Internet* (editado por Frank Schmalleger), Pearson Prentice Hall, New Jersey, 2008, p. 6.

¹²³ Sobre o assunto, Carlos Maria Romeo Casabona, Enrique Rovira Del Canto e Danielle da Rocha Cruz apresentam o novo bem jurídico como sendo a “*informação informatizada*”. CRUZ, Danielle da Rocha. Op. cit., p. 28.

A necessidade de estipulação de valores como os da integridade, disponibilidade e confidencialidade do meio ambiente informático faz com que se limite a esfera de atuação do Direito Penal ao mínimo necessário no ambiente virtual que prima por sua liberdade, sem paternalismos desnecessários. Então, para fins de clareza quando ao estudo em tela, é de se definir delito informático a partir de seu objeto de proteção.

UMA NOVA DEFINIÇÃO DE DELITO INFORMÁTICO

Considerando-se as prévias definições de crimes informáticos, a classificação optada (delitos informáticos próprios – puros e impuros – e delitos informáticos impróprios) e também o fato de que três são os elementos que compõe a segurança informática, tem-se que há necessidade do estabelecimento de definições para que então se possa dar prosseguimento ao estudo com mais profundidade.

Inicialmente, é de se apontar que a nomenclatura “crime informático” é deveras arriscada, levando-se em conta que a polícia tem investigado pessoas que se utilizaram de cassinos virtuais e até mesmo jogo do bicho virtual, tipificando-os nas contravenções penais dos artigos 50 e 58 do Decreto-Lei 3.688/41 (Lei das Contravenções Penais). Por tal motivos optou-se pela nomenclatura “delito informático”.

Delitos informáticos impróprios são delitos comuns, portanto condutas típicas, antijurídicas e culpáveis, e que são perpetradas utilizando-se de mecanismos informáticos como ferramental, sendo que outros meios poderiam ter sido igualmente eleitos para a prática.

Por sua vez, delitos informáticos próprios são as condutas típicas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade.

Conforme Rossini, delito informático pode ser tido como qualquer conduta constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com uso da informática em ambiente de rede ou fora dele, e que ofenda os

elementos da segurança informática¹²⁴.

CARACTERÍSTICAS DO DIREITO INFORMÁTICO

A partir da ideia de que há um novo paradigma a ser estudado, é fundamental que se verifique que, apesar de novel, há padrões que regem as novas condutas surgidas do novo ferramental e seus bens jurídicos inerentes e particulares. Desta feita, para que melhor compreenda-se os parâmetros a serem enfrentados nas investigações e nos processos crime, buscou-se raciocinar uma série de características especiais aplicáveis nesse ramo do Direito Penal.

Os delitos informáticos exigem algumas regras padrão a partir das quais todo o raciocínio jurídico-penal se monta e a partir da quais emanam características que se aplicam a todo um cabedal de condutas. São elementos a partir dos quais nascem os fenômenos atinentes à violação da segurança informática ou à nova ferramenta para lesionar de maneira inovadora os basilares bens jurídicos.

A partir de nosso estudo concluímos que são características da delinquência informática: a) a interatividade, b) a mobilidade, c) a conversabilidade, d) a conectividade, e) a ubiquidade, f) a globalização, g) a fracionabilidade, h) a divisibilidade, i) a intangibilidade, j) a disponibilidade, k) a pluralidade, l)) a velocidade, e m) a não territorialidade.

INTERATIVIDADE

A informática naturalmente pressupõe participação humana. Ainda que se diga que este é o ramo do saber que cuida do trato automatizado de informações, em verdade este trato só se dará a partir de uma ordem de um usuário, um comando. O raciocínio que se faz é idêntico ao da calculadora, que faz uma operação aritmética instantaneamente e sozinha, porém requer que alguém insira os dados em sua plataforma para que, somente após a ordem, o cálculo seja

¹²⁴ ROSSINI, Augusto Eduardo de Souza. Informática, telemática e Direito Penal. Memória Jurídica Editora. São Paulo. 2004. pp. 109 e 110.

feito.

Um robô, o computador ou o telefone celular cumprem com sua função de programação (andar, acessar a rede mundial de computadores, enviar uma mensagem de vídeo) após seu usuário dar-lhe o comando para tanto¹²⁵.

É conclusivo que o ambiente informático é de total interação com o usuário que o utiliza, em verdade requerendo *sine qua non* a prática de comandos para que as funções automatizadas se processem¹²⁶.

Mais do que isso, o ambiente informático permite que diversos usuários interajam ao mesmo tempo, cada qual fornecendo comandos diferenciados e, assim, solicitando que a tecnologia responda com aquilo desejado pelo ser humano. A interação de mais de um usuário em um mesmo ambiente faz com que se esteja virtualmente “em contato”, havendo, desta maneira, relacionamento.

Desta maneira, é natural o entendimento de que a informática e seus sistemas sempre serão meios para os quais fins estão programados. O sistema de *Internet banking* tem como finalidade o controle de contas bancárias, investimentos e outros serviços bancários, exclusivamente. Foi projetada para que seja possível ao indivíduo acessar sua própria conta (ou alguém por ele autorizado) com intenções legais ou ilegais, dependendo somente de seu juízo de valor.

Com isso, é de se compreender que qualquer atitude que ocorre na rede ou em

¹²⁵ Os japoneses desenvolveram um robô que serve cerveja e chopp como se fosse um barman, de maneira muito próxima do ideal. Contudo, ainda que a tecnologia tenha trazido vantagens e simpatizantes, ainda exige-se que o robô seja controlado remotamente por um ser humano, que dá as ordens. <http://g1.globo.com/Noticias/Tecnologia/0,,MUL635073-6174,00.html>. Acesso em 30.07.08 às 20:03hs.

¹²⁶ As três leis da robótica desenvolvidas por Isaac Asimov em seu romance “Eu, Robô” têm pertinência nesta etapa da exposição, muito especialmente a segunda delas. Isso porque de acordo com o autor, a única forma através da qual se poderia haver inteligência artificial (aqui interpretada como a informática, *mutatis mutandi*) seria a partir do obedecimento dos seguintes axiomas: 1ª lei: Um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum mal; 2ª lei: Um robô deve obedecer as ordens que lhe sejam dadas por seres humanos, exceto nos casos em que tais ordens contrariem a Primeira Lei; 3ª lei: Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a Primeira e Segunda Leis. Uma quarta lei foi inserida pelo próprio autor, em momento futuro, denominada Lei Zero, que diz “um robô não pode prejudicar a humanidade ou, através de omissão, permitir que a raça humana se fira”. Fonte: http://www.robotics.utexas.edu/rrg/learn_more/history/. Acesso em 02.01.09 às 00:35hs.

ambientes informáticos, obrigatória e necessariamente tem como ponto de partida um comando humano (permissão, negação, etc), ou uma programação prévia, não sendo possível que qualquer aparato pratique condutas a partir de juízo de valor próprio até o momento. Há carência de inteligência artificial autônoma, requerendo, qualquer ação na informática, um elemento volitivo humano.

Até mesmo os ataques de DoS (*Denial of Service* ou negação de serviço) que aparentemente são feitos por milhares de computadores automaticamente, em verdade nada mais são do que infecções simultâneas de milhares de máquinas, permitindo que um usuário mal intencionado escravize computadores alheios e busque, a partir de um comando seu (interação), que todos logrem acesso simultaneamente a um mesmo sítio eletrônico, provocando colapso por incapacidade de processamento simultâneo.

MOBILIDADE (ou PORTABILIDADE)

Esta é uma característica que vem sendo desenvolvida e cada dia torna-se maior tendência no mercado informático. A miniaturização dos componentes eletrônicos levou ao surgimento da microcomputação¹²⁷ que hoje permite que os antigos computadores que tinham o tamanho de uma sala, hoje sejam facilmente transportáveis ou até mesmo sejam primariamente móveis, como é o caso dos *palmtops*, *notebooks*, e, certamente, os telefones móveis (celulares).

Somado à portabilidade dos aparatos, encontra-se o fato de que o desenvolvimento de tecnologias de satélite, ondas de rádio (p. ex., *bluetooth* e infravermelho) e tecnologias populares e empresariais de acesso sem fio (*wi-fi* e *wi-max*, por exemplo) permitiu que tais dispositivos, além de processarem informações de maneira móvel, também pudessem conectar-se uns aos outros e à rede, sem limites ou restrições.

Desta maneira, a primária ideia de que o número de IP de uma máquina conectada à

¹²⁷ Em verdade o primeiro e decisivo passo para a microeletrônica, de acordo com Manuel Castells, foi dado em 1957 com a invenção do circuito integrado por Jack Kilby, engenheiro da Texas Instrument, em parceria com Bob Noyce. CASTELLS, Manuel. *A Sociedade em Rede*. 10ª Edição. Editora Paz e Terra S/A, São Paulo, 2007, p. 77

Internet levaria ao reconhecimento de um local físico tem perdido força, não podendo ser tido como uma premissa absoluta.

Tal característica ainda não está presente para a maioria dos usuarios, mas como tem sido tendência tecnológica o aumento da velocidade de conexões, a redução da dependência da tecnologia com fios e a convergência de funcionalidades informáticas para uma máquina somente (o aparelho celular móvel, hoje multifuncional), o aparecimento de tecnologias como a terceira geração de telefonia móvel leva aos usuarios a possibilidade de estarem conectados à rede a qualquer momento, e em qualquer local com cobertura. Suas ações dentro da rede, então, passam a poder ocorrer nos mais diversos lugares exigindo-se exclusivamente um acesso.

CONVERSABILIDADE

Expressão traduzida do inglês “*talkability*”, representa a capacidade dos aparatos informáticos em comunicarem entre si, graças à tendência de uniformização da linguagem e da possibilidade de diferentes tecnologias interagirem entre si, completando-se. Assim, a impressora de uma marca funcionará com aparelhos de qualquer marca, com diferentes sistemas operacionais. Também, diferentes *softwares* de navegação conseguirão compreender a linguagem da rede e serão hábeis para o acesso à rede mundial de computadores.

A habilidade de os aparelhos informáticos conversarem entre si faz com que haja condições de haver troca de informações, e, desta feita, troca de comandos entre aparelhos diferentes, levando-se, pois, a possibilidade de o usuario de um aparelho, em paridade com outro, acesse-o, visualize suas informações e até mesmo controle-o remotamente¹²⁸.

Os arquivos criados com o uso dos mais diversos programas são transmissíveis pela rede e chegam a um destinatário. Contudo diversos arquivos são específicos e somente podem ser abertos, visualizáveis e utilizáveis através de certos programas. Por sua vez, esta realidade

¹²⁸ A linguagem padrão que permite que os dispositivos conversem entre si chama-se Protocolo TCP/IP. É esta a linguagem utilizada mundialmente para que a rede tenha acesso universal. Entretanto, não podemos confundir a linguagem utilizada pelos aparelhos com a linguagem usada na rede mundial de computadores.

é indiferente quando se trata de comunicabilidade. Independentemente de se conseguir que o arquivo transmitido e recebido seja funcional, o envio e a chegada ocorrerão e isso se dá pela “*talkability*” da rede ou dos aparatos como telefones móveis.

A partir dessa característica conclui-se que não há relação entre delitos informáticos como de violação, intrusão ou contágio e as espécies de aparelhos envolvidos. Um cartão de memória de aparelho celular pode carregar um vírus que será inserido em um computador, ou uma impressora em rede pode ser acessada ilegalmente por uma máquina fotográfica com capacidade de conectar-se.

CONECTIVIDADE

A conectividade é a capacidade tecnológica que um aparelho tem de se conectar com outros aparelhos e/ou com a rede, como possível consequência¹²⁹. Não é uma característica de todos os equipamentos informáticos, mas a grande maioria dos novos aparelhos (filmadoras digitais, geladeiras, etc) têm sido fabricados com tal capacidade, no intuito de permitir o acesso à rede mundial de computadores e até para eliminar o uso de fios para a intercomunicação de aparelhos.

Para que dois ou mais aparelhos se conectem, há a necessidade de conversabilidade e de pareamento dos itens. Desta forma, a conexão entre computadores depende de ambos falarem a mesma linguagem e serem capazes de se compreenderem. Também, é fundamental que o usuário de um dos dispositivos solicite conexão a outro usuário que, por sua vez, tem a tarefa de aceitar ou não a ligação integrada. Uma vez conectados, pode-se dizer que há comunicação entre os dispositivos e, então, troca de dados.

De regra, esta é a forma como dispositivos conectam-se. Há, todavia, formas de se conectar a aparelhos informáticos explorando brechas de segurança, tomando conta da programação de um computador ou similar conectado e até mesmo enganando o usuário que, acreditando que a conexão (ou o pedido de conexão) é confiável, termina por autorizar em erro

¹²⁹ A rede está disponível a partir da conexão feita a um computador que tem como função fazer a filtragem, autorização e a ponte entre a rede mundial de computadores e cada usuário conectado, registrando a

o pareamento dos itens¹³⁰.

MUNDIALIZAÇÃO

A informática e seus segmentos de aplicação foram responsáveis pela figura do dito “cidadão do mundo”. A concepção da “rede das redes” derrubou barreiras geográficas, dando a qualquer usuário o poder da informação, o poder de visitar locais antes exclusivos, próximo do desejo de conhecimento e distante da xenofobia, das dificuldades financeiras e afins.

O conceito de mundialização poderia ser substituído pelo de popularização da rede, uma vez que anualmente tem-se notado aumento do número de pessoas denominadas conectadas. A tendência da rede, oferecendo a cada dia mais ferramentas gratuitas e aumentando a capacidade de armazenamento é ter adeptos mais frequentes.

Ao relacionarmos-nos, seja comercial seja pessoalmente, com um usuário da informática, com um internauta ou com pessoas jurídicas em rede, sempre resta uma sensação mista de proximidade somada à de incerteza quanto à localidade de onde partiu o acesso.

Por um lado acredita-se sempre que o relacionamento virtual dá-nos mais intimidade com o interlocutor, uma relação mais pessoal e dedicada. Por outro lado, um pensamento mais detido leva-nos à cautela e insegurança, partindo-se da premissa de que não há fronteiras para

hora de início e fim da atividade.

¹³⁰ O pareamento é o ato pelo qual dois dispositivos não conectados passam a conectarem-se e trocam informações por conta de sua compatibilidade, comunicabilidade e porque um deles solicita ao outro autorização para tal sincronismo e que é aceita pelo outro aparato, automaticamente ou através de um comando de seu usuário. A partir de tal ligação, dados podem ser compartilhados, programas podem ser utilizados conjuntamente e até mesmo recursos podem ser utilizados pelo usuário que se conectou. O termo pareamento é oriundo da expressão norte-americana *pairing*, que, por sua vez, é uma verbalização do adjetivo “*pair*” que significa “par”. Tal expressão tem tal natureza pelo fato de que a comunicação geralmente se dá entre dois aparelhos, sendo um solicitante da conexão e o outro aceitante do pedido de conexão alheia. Portanto e naturalmente, há que se ter de regra dois dispositivos interligados e comunicantes para que ocorra a troca de informações. Importante se notar que qualquer conexão à Internet pressupõe o pareamento de máquinas. Para que uma máquina obtenha acesso à rede mundial de computadores, por exemplo, inicialmente ela terá que ser capaz de se comunicar com uma máquina do provedor desse serviço, que o legitima e reconhece através de uma senha de usuário e, a partir de tal autorização, mantém-no conectado. A perda de tal pareamento implica em imediata perda de conexão, ou seja, a perda da ligação do aparato garantidor de acesso à rede e o aparato solicitante de conexão.

o contato entre pessoas e que quaisquer envolvimento podem gerar consequências jurídicas com apuração duvidosa, trazendo o sentimento de fragilidade e super exposição, visto que o contato feito entre pessoas na mesma cidade ou em diferentes hemisférios do planeta ocorre da mesma forma e com a mesma velocidade.

Aos comerciantes, a rede mostrou-se altamente vantajosa: alcançam hoje e promovem *marketing* a um numeral muito maior de potenciais consumidores a um preço baixo e com penetração a lares e ambientes de trabalho. Os custos da comunicação à distância, as barreiras geográficas e a linguagem por muito foram responsáveis pelas ações pontuais e concentradas dos fornecedores, que eram obrigados a relacionar-se em células de atuação. Hoje, um sítio eletrônico pode ser indistintamente acessado por milhões, bastante um acesso à rede.

Aos usuarios particulares, também imensa capacidade de cultura, leitura de jornais, revistas, filmes, fotografias, curiosidades, conhecimento científico imediato, até mesmo a possibilidade de aplicação na bolsa, compras sem barreiras, jogos virtuais, músicas ilimitadas, enfim, a quantidade de material produzido por todo o mundo passa a poder ser acessado sem restrição, especialmente pela disseminação da língua inglesa como a principal na rede.

Contudo, a diminuição das dificuldades de relacionamento a distância gera uma vulnerabilidade crescente. Enquanto que em tempos remotos uma pessoa mais simples e interiorana preocupava-se com a conduta do próximo ao ir para cidades grandes por lá estarem os delinquentes e estelionatários, a mundialização das relações fez com que no mundo virtual não houvesse limites para a incidência de tentativas de golpes: basta se estar conectado na rede e se está propenso a violências e agressões virtuais. Observe-se o que diz o contrato de prestação de serviço da empresa Google, ao propor seus serviços:

“O usuario compreende que, ao utilizar os Serviços, pode estar exposto a Conteúdo que possa considerar ofensivo, indecente ou censurável e que, a este respeito, utiliza os Serviços por sua conta e risco”¹³¹

¹³¹ No original, “8.4 You understand that by using the Services you may be exposed to Content that you may find offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk”.

Por isso, há que se compreender que ainda que vivamos num mundo com línguas e culturas particulares para cada soberania, no que se refere à contato ou potencialidade de interação entre hemisférios, países e regiões, a tecnologia retirou o caráter restritivo das fronteiras, garantindo que qualquer episódio ocorrido em qualquer localidade do planeta seja imediatamente conhecido por todos os países conectados, num misto de contaminação e interação. Em verdade, canais de informações para o mercado financeiro mundial como o *Bloomberg*, além de mídias jornalísticas já preponderantemente prevalecem em seus acessos através da informática por serem mais dinâmicos e poderem ser utilizados conforme a necessidade do usuário¹³².

Portanto, são características da informática sua dinâmica e crescente disponibilidade ampla para o ambiente virtual, ganhando velocidade na troca, com grande e ilimitada abrangência e divulgação.

FRACIONABILIDADE

Um dos pontos fundamentais para a compreensão da delinquência informática está no fato de que dados são fracionáveis, ou seja, podem ser reduzidos a pedaços de programação. Com isso, é de se entender que os arquivos economicamente relevantes são longas cadeias de significados e é correto apontar-se para o fato de que não existem dados dessa modalidade que não sejam compostos por diversas porções de linhas de programação.

Seriam, os dados, metaforicamente, como uma blusa de tricô em que cada nó e cada linha são fundamentais para sua constituição, individualmente, sob pena de ruir seu objetivo. Assim como a blusa de lã com uma de suas linhas incorretamente tricotada tenderá a desfiar e perderá sentido, o mesmo ocorre com os dados informáticos: exige-se que as linhas estejam

¹³² *Link* para o arquivo de áudio do programa “Notícia em Foco” da rádio CBN – Central Brasileira de Notícias em que jornalistas discutem a condenação dos jornais de papel por conta da digitalização das mídias jornalísticas e disponibilização na Internet. Participação do convidado Rosental Calmon Alves, diretor-fundador do Centro Knight para o Jornalismo nas Américas, na Universidade do Texas, em Austin. http://cbn.globoradio.globo.com/cbn/wma/player_gradio.asp?audio=2008/colunas/noticiafoco_081110.wma&OAS_sitepage=sgr/sgr/radioclick/radiosam/cbn/noticiaemfoco1. Acesso em 21.11.08 às 19:53hs. No mesmo sentido, entrevista com o jornalista Lourival Sant’Anna, autor do livro “O destino do Jornal” em <http://observatorio.ultimosegundo.ig.com.br/artigos.asp?cod=493IMQ002>. Acesso em 21.11.08 às 19:55hs.

corretas para que seu significado e sua leitura também o sejam.

Isto posto, a possibilidade de modificação de apenas uma parte de um arquivo de dado é plena, até mesmo se adicionando linhas de programação (como no caso de um arquivo que ao ser copiado para um aparelho inicia um processo de replicagem constante), se retirando linhas de programação (tornando o arquivo ilegível pelo aparato) e até mesmo modificando linhas de programação (mudando, por exemplo, a fórmula utilizada para resolver um cálculo, gerando erros)¹³³.

Assim, num quebra-cabeças, a falta de uma peça leva à total inutilidade, levando todo o esforço para um despropósito; o mesmo ocorre com um arquivo de dados. A falta de uma linha ou um caractere da programação poderá levar a geração do arquivo para uma inocuidade informática.

Acrescer peças num quebra-cabeças, contudo, é um despropósito, assim como modificá-las. Todavia, no processamento de dados isso é possível: conhecedores da linguagem podem modificar partes da programação levando um arquivo ou comando a agirem de forma diversa da original.

Diante dessas características, é correto afirmar que arquivos, dados e comandos podem ter sua integridade atacada, gerando resultados danosos, muitas vezes mascarados e veiculados ardilosamente.

DIVISIBILIDADE

O sentido a ser dado nesta característica não é o mesmo do dado à fracionabilidade.

¹³³ Conforme evoluem as capacidades de processamento de dados – seja pela maior velocidade dos processadores, seja por sua multiplicidade –, mais forte fica a capacidade de ler arquivos de dados mais complexos, com boa velocidade. Por isso, as tecnologias acessórias – *scanners*, máquinas digitais de fotografia, arquivos de áudio, etc –, contando com tal evoluir de tolerância a dados mais pesados e de mais qualidade, leva os arquivos de dados a crescerem de tamanho (*rectius*, volume de dados). O crescimento em complexidade e qualidade leva a maior quantidade de linhas de programação que deverão ser lidas e interpretadas pelo maquinário. Da mesma forma, os dispositivos criadores de tais arquivos devem ter grande habilidade de processamento, pois que os arquivos aumentam de tamanho e complexidade mas não toleram que sua escrita tenha qualquer erro, para que haja plena funcionalidade.

Enquanto que esta existe ligada à ideia de composição dos dados e à sua segmentação, inerente à programação, a divisibilidade, por sua vez, está diretamente relacionada com a forma como estes são transferidos na rede mundial de computadores.

Para que se consiga ter acesso à rede, já se disse, faz-se necessário que haja uma conexão entre um usuário (público ou privado, pessoa natural ou jurídica) e um provedor. Tal acesso é garantido pela capacidade de os dispositivos se conectarem e conversarem entre si através de trocas constantes de comandos e dados.

Também, é conhecimento pressuposto o de que dados são, em verdade, linhas de programação que se agrupam e são quantificadas de acordo com sua complexidade, em unidades de *bits*. Assim já explanado, caractere por caractere, linha por linha, a programação como um todo leva à criação de um arquivo que passa a ter algum valor a partir de seu significado quando interpretado por um aparato informático e traduzido para a capacidade humana de compreensão.

Porém, a quantidade de dados que se troca ao longo de relações informáticas é muito grande e crescente a cada ano. Para que, exemplificativamente, alguém cheque seu *email* fornecido como um serviço gratuito de uma marca, é necessário que toda a interface necessária para tanto seja carregada no computador do usuário¹³⁴.

O que ocorre é que as linhas que transmitem os sinais da rede – eletricidade, cabo, fibra ótica, ondas de rádio, etc – não estão livres de cometerem erros de transmissão e/ou sofrerem falhas técnicas ou até mesmo interrupção de funcionamento. E este foi o pensamento que deu margem à criação da Internet como uma rede difusa.

Também, somada à capacidade natural de erros e dificuldades na transmissão dos dados está a limitação quanto a capacidade de transmissão das tecnologias frente à possíveis

¹³⁴ Há, pois, que se dar um comando prévio para que o respectivo *site* em que se encontra o serviço de *email* seja carregado no computador do detentor da conta e seja exibido em sua tela. Ao se digitar no campo do navegador o endereço do serviço, um comando é dado ao computador que fornecerá o serviço. Este computador contém os dados referentes às cores que aparecerão na tela, os campos a serem preenchidos, as publicidades veiculadas, e assim por diante. Dado o comando, um pedido para que todos os arquivos necessários para se carregar a interface é dado. A resposta será o envio dos dados necessários, que devem ser perfeitos para que a exibição seja, também, correta e perfeita.

sobrecargas das vias¹³⁵.

O fato de a Internet ser difusa faz com que os dados tenham inúmeros caminhos diferentes para atingirem o mesmo destino, todos igualmente viáveis e aptos. Também, uma vez que se trata de transmissão de dados na velocidade da luz, o cumprimento de vias que os dados precisariam trilhar até atingir o destino é praticamente irrelevante.

A partir de ambas premissas – a de que a transmissão de dados está sujeita a erros diversos e a de que as vias de conectividade tem capacidade de transmissão limitada – foi que a informática desenvolveu a forma de transmissão de dados que se chama de transmissão por pacotes de dados.

Uma vez que há fracionabilidade dos dados e que há ordem correta para que as linhas de programação estejam compostas para haver significado, surge a possibilidade de promover “cortes” nos arquivos com a criação de diversos trechos de programação sem significado sozinhos, mas que, reagrupados com outros trechos adequados referentes ao arquivo fragmentado, voltam a compor o arquivo integral, agora transmitido para outro local da rede¹³⁶.

¹³⁵ A fibra ótica tem capacidade de transmissão de dados até 1 milhão de vezes maior do que o cabo metálico. Ocorre que praticamente não há diferença entre a velocidade de transmissão em um cabo metálico e a fibra. O que muda é a capacidade de transmissão. A fibra pode transportar um número muito maior de *bits* por segundo do que o cabo. Comparativamente, a ideia seria a de evacuação de um prédio comercial por uma porta simples ou por diversos portões. Fonte: <http://www.terra.com.br/reporterterra/fibra/material1.htm>. Acesso em 03.08.08 às 21:00hs.

¹³⁶ Tal técnica traz vantagens e dificuldades. As duas principais vantagens são quanto à eficiência e quanto à velocidade de transmissão. A eficiência está no fato de que a divisão de arquivos em blocos faz com que as remessas vão sendo feita de maneira gradual e consistente: terminado o envio de um bloco, está consolidado aquele bloco de informações, que fica armazenado, aguardando o recebimento dos blocos sucessivos até que todo o dado esteja transmitido. A perda de envio de um trecho dos dados não compromete o envio de todo o arquivo, que pode ser retomado de acordo com a conclusão de blocos. E cada bloco ou pacote remetido traz em si a quantidade de pacotes que compõe todo o arquivo de dados. Desta forma, o dispositivo receptor processa, a cada bloco recebido, se todos os pacotes necessários para a leitura de determinado dado foram recebidos. Se sim, cessa-se a transmissão; se não, o dispositivo receptor informa o emissor que houve falha e este remete novamente os pacotes, tantas vezes quantas forem necessárias, até que a operação se aperfeiçoe. No que se refere à velocidade, os ganhos também são latentes. Se a rede é composta de inúmeras rotas ou caminhos alternativos que fazem com que os dados cheguem até um mesmo destino, com a mesma velocidade, nítido é que a divisão em pacotes e o envio simultâneo de tais pacotes faz com que a velocidade seja potencializada, tendo-se em vista que ao invés de se remeter todos os arquivos um a um pela mesma rota, com os riscos de erro e com a possibilidade de erros, pode-se remeter rapidamente todos de uma só vez.

Tendo-se em vista que a máquina receptora é capaz de processar o recebimento de todos os pacotes com imediata leitura da ordem com que devam ser agrupados e a montagem do arquivo, é mais vantajoso que diversas rotas

Um ponto juridicamente importante é a praticamente impossibilidade de controle dos caminhos percorridos pelos pacotes até chegarem a seus destinos, podendo passar por Estados soberanos diferentes, com regras diversas acerca de, por exemplo, pornografia ou direitos autorais.

A divisibilidade também acaba por ser importante no estudo do Direito Penal informático, tendo-se em vista que o tráfego dos pacotes de dados é livre pela rede, sujeito a interceptação e feito de forma repetida e incontrolável até que o destino receba os arquivos necessários. Isso faz com que, primeiramente, possa haver interceptação de dados durante sua transmissão e, em segundo plano, que tais interceptações se dêem em soberanias em que não há previsão legislativa para coibir tais práticas – o que geraria uma permissão para a captura de tais dados.

Também se mostra importante a divisibilidade pois ao mesmo tempo que denota aumento de velocidade, explicita uma fragilidade da rede: a limitação de transmissão e processamento de dados (restrita a pacotes pequenos de dados), fato que leva usuários mal intencionados a provocarem verdadeiros boicotes em certos serviços, sobrecarregando certas vias de acesso, obstruindo certos *sites* com bombardeamento de comandos de envio e recebimento de pacotes de informações, levando a sobrecargas e indisponibilidade.

INTANGIBILIDADE

Conforme anteriormente explanado, é inerente ao conceito de informática a criação, utilização e troca de dados permanente. Os dados podem ser informações sobre a interface do programa em execução, o arquivo de texto criado, a planilha de custos da empresa e até mesmo o *email* remetido para alguém. De qualquer maneira, todos esses dados têm um ponto

sejam utilizadas razoavelmente para transporte ao invés de uma ou poucas somente, com possibilidade de sobrecarga. Assim, a rede acaba por equilibrar a transmissão de dados, inclusive podendo, em percebendo uma rota congestionada ou com falha técnica, reordenar o envio dos dados por caminhos alternativos. As dificuldades de tal técnica estão no fato de que a remessa de arquivos em bloco exige que o agrupamento dos blocos de dados seja perfeito para que os arquivos cheguem com possibilidade de serem compreendidos e traduzidos para o usuário. Com isso, não raro a remessa do arquivo e de seus diversos pacotes pode se dar dezenas de vezes, sendo que os segmentos que não forem recebidos ou processados acabam por carregar a rede de espécies de “lixos virtuais” que seriam os pacotes enviados, que ocupam espaço de transmissão, mas que não tem ou terão uso na rede.

em comum: não são materiais e nem são materializáveis por si. Os dados tratados pela informática nada mais são do que *bits* interpretados por dispositivos.

A sociedade pós-industrial evoluiu e passou a criar um novo produto com altíssimo valor: a informação. Com a migração da mão-de-obra para o setor terciário, de serviços, e com o evoluir tecnológico para instrumentos de trabalhos focados em trato de informação, a sociedade passou a investir em uma espécie de círculo virtuoso. O informacionalismo, pois, tem como modo de desenvolvimento a busca pelo desenvolvimento tecnológico, ou seja, a acumulação de conhecimentos e maiores níveis de complexidade do processamento da informação, que, por sua vez geram maior conhecimento e assim sucessivamente¹³⁷.

Uma vez que os dados produzidos a partir da informática passam a ter valor real, portanto, conclui-se que os *bits* agrupados tornam-se bens juridicamente relevantes. Contudo, a imaterialidade dos novos bens é óbvia.

Por força do artigo 2º da Lei 9.609/98, programas de computador têm o mesmo regime de proteção jurídica que direitos autorais que, assegurados pelo artigo 3º da Lei 9.610/98 devem ser considerados bens móveis. Verifique-se que a definição de programa de computador adéqua-se à ideia de dados em geral, uma vez que programa nada mais é do que uma enorme sequência de dados programados¹³⁸ para determinada função e que é apresentada como:

“Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e

¹³⁷ CASTELLS, Manuel. A Sociedade em Rede. Volume I. Editora Paz e Terra S/A. 2007. Rio de Janeiro. p.54

¹³⁸ Ao se obter um arquivo com significado econômico a partir de uma programação o que se está fazendo é agrupando uma sequência de comandos que poderão ser acessados e produzir efeitos quando interpretados por um dispositivo. Esta sequência de comandos fica armazenada em arquivos, que por sua vez nada mais são do que blocos organizados de comandos a serem interpretados por um aparato e transformados em linguagem compreensível para o ser humano, em regra.

*para fins determinados.*¹³⁹”

Ocorre que os *bits* podem conter a representação digital de documentos importantes, obras artísticas, investimentos financeiros, agenda de telefones, dentre tantos outros dados importantes e que podem ter muito valor comercial se corretamente utilizados.

Ora, vê-se que os dados são simultaneamente algo que satisfaz a necessidade humana e, por agregarem valor, por terem função, acabam por merecer a proteção do Direito¹⁴⁰.

Contudo, dados são criações humanas, fruto da inventividade e da compreensão de sinais necessários¹⁴¹. São, pois, obras originais, imateriais, intangíveis, existentes somente alocadas em um suporte material, que o grava por meios físicos, químicos, magnéticos ou outros. Por conta dos símbolos que se formam da tradução da programação, os dados passam a ter significado e tais significados, muitas vezes representam ideias e conteúdos com valor pecuniário, constituindo-se verdadeiro patrimônio. Paralelamente, é de se entender que as ideias pertencem a seus autores que podem explorá-la e contam com a proteção do direito.

A característica da imaterialidade mostra-se bastante peculiar pois leva a uma forte dificuldade de adaptação das regras já existentes atinentes a delitos que violam patrimônio e, portanto, gera uma necessidade de legislação especial.

Crimes como o de furto ou roubo, exemplificativamente, exigem que o bem jurídico afetado seja o patrimônio materializado na forma de coisa, portanto, um objeto material. Some-se a isso o fato de que por conta da característica da pluralidade (abaixo descrita com maior minúcia) não é possível que haja a subtração de um dado, visto que na informática as técnicas utilizadas chamam-se replicagem, ou seja, não se subtrai um bem imaterial informático, mas sim se copia um idêntico e, quiçá, se apaga a fonte da cópia.

¹³⁹ Artigo 1º da Lei 9.609 de 19 de fevereiro de 1998.

¹⁴⁰ Exemplo da proteção merecida por bens jurídicos advindos da informática são as leis nº 9.609 – que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências – e nº 9.983 – que inseriu os tipos de inserção de dados falsos em sistema de informações, modificação ou alteração não autorizada de sistema de informações, dentre outros

¹⁴¹ O filósofo Cícero faz uma interessante divisão quando diz que há coisas que existem (*quae sunt*) e outras que se concebem (*quae intelleguntur*). Os dados seriam coisas concebidas pelo intelecto. *Apud* NERY JR, Nelson; NERY, Rosa M. de A.. **Código civil comentado**. 4.ed. São Paulo: RT, 2006. p. 690.

Certamente, também, a intangibilidade dificulta sobremaneira a percepção imediata da violação de dados pelas vítimas porquanto tais bens não ocupam espaço físico nem quando armazenados.

Ainda tratando da característica, é de se destacar o fato de que se tendo em vista serem os dados imateriais e, portanto, impalpáveis e de difícil percepção, ataques a tais bens móveis serão comumente da mesma natureza, ou seja, virtuais, sendo a máquina do usuário-alvo sujeita a receber arquivos de dados com códigos maliciosos que darão ao dispositivo comandos prejudiciais a seu proprietário.

DISPONIBILIDADE

A disponibilidade foi apontada previamente como um dos elementos da segurança telemática. Trata-se da possibilidade de o legítimo detentor dos direitos de acesso a determinado serviço, funcionalidade, arquivo ou programa fazê-lo a qualquer momento que dele *necessite*, sem embaraços.

Assim, a informática existe a serviço do homem e no intuito de auxiliá-lo como ferramental para as tarefas que dele *necessitem*. Ocorre que o evoluir da informática trouxe a característica da conectividade dos dispositivos entre si ou com a rede mundial de computadores, o que influenciou diretamente na ideia de disponibilidade.

Primeiro pelo fato de que a conectividade é uma via de duas mãos. Ao mesmo tempo em que um usuário está conectado por sua iniciativa (conexão ativa), está também sujeito a ser conectado (conexão passiva) e da mesma forma que remete arquivos e envia comandos, os recebe. A sujeição quanto a recebimento de arquivos se dá por conta da conexão revelar-se uma porta aberta do usuário, permitindo interações tanto benéficas quanto maléficas.

Dentre as possíveis remessas maléficas, estão as de arquivos que prejudicam o acesso a dados, a conexão da máquina com a rede mundial de computadores, e até mesmo arquivos que dão controle da máquina a terceiros ou permitem a colocação ou modificação de senhas desconhecidas. Com base nos exemplos, conclui-se que a conectividade influenciou sobremaneira a característica da disponibilidade fazendo com que fosse possível sua restrição.

Outro ponto é que a conectividade abriu novos horizontes para a criação e desenvolvimento de arquivos e programas feitos exclusivamente dentro da rede, a partir do conceito de Web 2.0 e Internet como nuvem. Também, alguns serviços como *e-mails* gratuitos, hospedagem de *sites*, discos rígidos virtuais, redes sociais e comunicação plural passaram a existir exclusivamente dentro da rede que coloca-se como exclusiva para a possibilidade destes usos.

A disponibilidade é, de maneira mais abrangente, a possibilidade não só de acessar os dados existentes na própria máquina do usuário como também a possibilidade de este ter acesso aos programas e serviços que contratou, gratuitamente ou onerosamente, na rede, e que são garantidos a partir do acesso prévio a um *site*.

Assim, a disponibilidade engloba também a possibilidade de o usuário conseguir que seu objetivo de uso de ferramentas *online* seja atendido quando deles precisar. Para tanto, a conta utilizada para acessar os *sites* de serviços deve estar disponível para que o usuário possa dela valer e, a partir dela, utilizar-se dos mais variados programas existentes, acessar sua caixa de mensagens, acessar um arquivo armazenado e assim por diante.

Ataques quanto à disponibilidade, podem ter duas espécies de alvo: o computador de um usuário individual, ou a fonte que provém serviços e na qual milhares de usuários ingressam e conectam-se.

Os objetivos dos delinquentes, por sua vez, também podem ser diferenciados, pois ataques a serviços podem ser formas de protesto de cibervândalos, ciberfundamentalistas, ciberterroristas e até mesmo descontentes; ataques individuais, por sua vez em regra são ataques que pretendem alguma espécie de vantagem pecuniária, vingança pessoal ou difusão de programas maliciosos desenvolvidos.

De qualquer maneira, a disponibilidade pode ser atacada com ação diretamente no dispositivo de outrem, (p.ex., a inserção de um *pen drive* infectado) ou pode ser atacada indiretamente, através do subterfúgio intermediário da conectividade (p.ex., envio de anexo de *email* contendo um *malware*). Ambas as formas ensejarão uma falta de possibilidade de o usuário utilizar de algum ou alguns de seus dispositivos, serviços, e isso fará com que a tecnologia informática perca seu principal mote: servir quem dela precise, no momento

necessário.

PLURALIDADE

A principal diferença existente entre o mundo tangível material e o mundo intangível virtual ou informático é sua composição. A matéria que compõe os bens corpóreos é única e formada de unidades denominadas átomos, que obedecem regras de ciências como física e química. Em contrapartida, na informática tudo é formado por *bits*.

Ainda que seja possível criar, em linha de produção, carros idênticos aos olhos leigos, em verdade, por mais similares que sejam jamais serão iguais pois que são formados por partículas atômicas diferentes. Por isso, cada objeto material é, em sua essência, puro e único¹⁴².

A partir de tal ponto, é certo afirmar que o conceito de propriedade tem aplicação diferente no mundo material e no mundo informático.

No mundo real, a propriedade é única. O conceito de fungibilidade está relacionado com bens com idênticas características, substituíveis em tese e porque qualquer deles, se parecido, atende à mesma função.

Contudo, é notório que uma propriedade destruída jamais será a mesma, visto que aquela que a substituirá será composta por outros átomos. Cada objeto material é, certamente um original único e insubstituível etiologicamente.

Dados, a *contrario sensu*, não são formados por matéria, mas sim por uma linguagem que pode ser traduzida por programas e sistemas competentes para tal tarefa. Não tem utilidade por si só, mas somente quando transformados numa linguagem compreensível ao ser humano.

Ocorre que qualquer aparelho informático com capacidade para transformar dados,

¹⁴² O mesmo raciocínio se aplica à clonagem. Mesmo que se consiga produzir espécimes com exatas mesmas características, átomos são exclusivos. Cada clone será composto por seus átomos de matéria e somente poderão estar em um lugar do espaço ao mesmo tempo.

traduzindo-os para seu usuário lê de maneira idêntica tal sequência de *bits*, fazendo com que o arquivo seja decodificado de modo idêntico, qualquer que seja o usuário.

Mais do que isso, os dados, por serem mera sequência de linguagem, podem ser replicados identicamente, pois que não são materiais. Qualquer réplica do original, portanto, tem exatamente as mesmas funcionalidades e poderá ser identicamente traduzido por um aparato sendo, desta feita e na realidade, um original.

Em outras palavras, há a possibilidade de existirem diversos arquivos originais, idênticos, e com as mesmas funcionalidades, pois que *bits* são imateriais e plurais. Decerto os detentores dos direitos sobre programas, fotos, filmes, e outros arquivos de dados, por não terem interesse em que seus direitos autorais sejam vilipendiados, criam mecanismos de proteção ou remuneração de cópias. E isso se dá exatamente pelo fato de que, sem tal proteção impeditiva, qualquer um pode deter qualquer dado, com todas as características de um original e mesmas atribuições.

Com isso, arquivos benéficos ou maléficos não têm limite para existirem de maneira plúrima, sendo que cada cópia será capaz de produzir os mesmos efeitos da original programada.

Também, é imprescindível compreender-se que por se poder existir uma infinidade de originais, o conceito de propriedade exclusiva não existe, podendo um arquivo idêntico ser propriedade de múltiplos usuários ao mesmo tempo.

UBIQUIDADE (ou SIMULTANEIDADE)

A ubiquidade, também denominada de simultaneidade e onipresença, está entre as características mais marcantes da informática, visto que guarda relação com bens intangíveis, assim como o direito autoral.

Certos Principios da mecânica não têm aplicabilidade ao pensarse na delinquência informática. Enquanto que em geral dois corpos não podem estar no mesmo lugar de espaço ao mesmo tempo, tal conceito não tem aplicabilidade na informática, por conta do Princípio da

não territorialidade ser aplicável a tais condutas¹⁴³.

Na informática, graças à conectividade, pode-se estar em diversos lugares virtuais ao mesmo tempo, independentemente da velocidade de sua conexão, da capacidade individual ou de barreiras físicas e políticas. E assim é a ubiquidade: a capacidade de se estar presente em diversos lugares ao mesmo tempo.

Um indivíduo pode estar no Japão, acessar um portal de informações em Los Angeles que o permite assistir vídeos que estão hospedados na Espanha mas que foram feitos por sul-africanos. Onde está o usuário? Somado ao conceito de velocidade, a ideia de que todos podem estar em diversos lugares ao mesmo tempo, processando dados diferentes, praticando condutas livres, é fundamental. E este conceito é aplicável na rede mundial de computadores, mas não se limita a ela.

A partir de tecnologias de conexão sem fios e à distância, uma pessoa pode conectar-se a um provedor a dezenas de quilômetros de distância, compartilhar arquivos através de ondas de rádio há muitos metros e a impressão é a de que o usuário está nos dois ou mais lugares ao mesmo tempo.

A sensação de simultaneidade é tamanha que a cada dia mais se busca profissionais capazes de gerir diversas informações, de naturezas diferentes, sem qualquer dificuldade. O conceito de simultaneidade, inclusive, trouxe ideias como a de participar de funerais à distância, controlar as câmeras de segurança de empresa ou casa à distância e até mesmo, através do celular, ligar a banheira da casa, para preparar um banho.

Tal conceito, ao mesmo tempo que gera uma fantástica sensação de multitudinarianidade, de multiplicação benéfica de funções e tarefas, ao mesmo tempo gera inseguranças, pois que alguém mal intencionado poderá, tal como qualquer usuário, buscar violar diversos bens jurídicos ou aferir vantagens sem o limite físico, contra vários usuários simultaneamente, ficando potencializadas as condutas.

¹⁴³ “(...) *there exists a fine line of demarcation between the crimes of physical space and crimes of cyberspace. The demarcation lies in the involvement of the cyber medium (Pati 2003), lack of geographical boundaries (Hafner and Markoff 1995; Mitra 1999), and their occurrence in a diffuse, fluid, evolving (Brenner 2004b) and spatiotemporally disorganized environment (primarily the collapse of spatial-temporal barriers, mani-to-many*

Por fim, há uma problemática quando se trata de ubiquidade de crimes informáticos, especialmente no que toca ao fato de que uma ação pode ser considerada crime em um país e não em outro, gerando-se, pois, conflito no que se refere à forma de repressão. Veja-se a posição de Karuppannan Jaishankar, professor da Universidade Manonmaniam Sundaranar na Índia, que desenvolveu a teoria da transação espacial para os cibercrimes¹⁴⁴, quando diz que:

*“A conduta em questão pode não ser ilegal. ‘Outra característica do cibercrime é que a conduta em questão pode não ser ilegal (Brenner 2001). Em maio de 2000, o vírus “Eu te amo” atravessou o mundo em duas horas e causou bilhões de dólares em danos em mais de 20 países. Ele foi rapidamente rastreado com origem nas Filipinas, onde agentes do FBI e autoridades locais identificaram um suspeito. Mas como a lei filipina não criminalizava a disseminação de vírus, levou-se dias para se conseguir um mandado de busca no apartamento do suspeito, dando-lhe tempo para destruir as evidências. E ainda havia o problema processual (...) tendo-se em vista que disseminação de vírus não era crime local, o suspeito não poderia ser extraditado para ser processado nos Estados Unidos, onde o fato era crime (...) ninguém nunca foi processado pela disseminação em tela.”*¹⁴⁵

No que se refere à competência para julgamento dos crimes informáticos, afora os ensinamentos do artigo 70 “caput” do Código de Processo Penal aplicáveis aos crimes

connectivity, and the anonymity and plasticity of online identity.” JAISHANKAR, K. Space Transition Theory of Cyber Crimes in Crimes of the Internet. Pearson Prentice Hall. New Jersey, 2008, pp. 290-291.

¹⁴⁴ JAISHANKAR, Karuppannan “Space Transition Theory of Cyber Crimes” in **Crimes of the Internet**. 1a. edição (editores SCHMALLEGER, Frank e PITTARO, Michel), 2008 New Jersey, Pearson Prentice Hall, pp. 283 a 301.

¹⁴⁵ “Conduct at issue may not be illegal. “Another characteristic of cybercrime is that the conduct at issue may not be illegal” (Brenner 2001). In May 2000, the “Love Bug” virus raced around the world in two hours and caused billions of dollars of damage in over 20 countries. It was quickly traced to the Philippines, where FBI agents and local authorities identified a suspect. But since Philippines law did not criminalize virus dissemination, it took days to get a warrant to search his apartment, giving him time to destroy evidence. Then there was the problem of prosecution. (...) since virus dissemination was not a local crime, he could not be extradited for prosecution in United States, where it was a crime. (...) no one was ever prosecuted for disseminating it”. JAISHANKAR, K. Space Transition Theory of Cyber Crimes in Crimes of the Internet. Pearson Prentice Hall. New Jersey, 2008, pp. 290-291

materiais, aos denominados crimes à distância, de modo geral¹⁴⁶, aplica-se a Teoria da Ubiquidade, interpretando-se, conforme NUCCI, os artigos 6º do Código Penal e os parágrafos 1º e 2º do artigo 70 do Código de Processo Penal. A partir dessa interpretação, conclui-se que basta parcela da execução do tipo ocorrida no Brasil para que seja aplicada a legislação pátria¹⁴⁷.

ANONIMIDADE

É característico da informática o fato de que as interações e relações são feitas entre aparelhos. Por sua vez, os aparelhos conectados são necessariamente operacionalizados por serem humanos. Contudo, a tecnologia é universal e pode ser utilizada por todo e qualquer indivíduo capaz de compreender seus meandros, sua linguagem e apresentar comandos a serem obedecidos.

Diante disso, entende-se que computadores trocam informações entre si, independentemente de quem esteja determinando suas funções. Não tem o ser humano médio a capacidade de compreender a linguagem pela qual o computador processa as informações e nem produzir as mesmas funções, necessitando do intermédio da máquina. Assim, a informática acaba por tratar da troca de dados entre os aparatos, estes sendo as pontas da relação comunicativa.

O usuário é um administrador de comandos a distância, operando um maquinário, mas que o faz de maneira velada, pois que desnecessária é sua exposição para a função. A ideia inicial da computação foi a de facilitação de tarefas para usuários, tendo surgido somente depois a concepção de relacionamento a distância. Desta forma, o principal cuidado do cientista foi o de fazer com que a capacidade de processamento de dados fosse ideal (e crescesse conforme necessidade) para que houvesse a substituição do homem.

Isso significa que foi restringida a função humana, em algumas tarefas, para, exemplificativamente, um apertar de botões a distância, poupando o ser humano, dando-lhe

¹⁴⁶ O artigo 63 da Lei 9.099/95 aponta exceção, pois que explicita a teoria da atividade como prevalente. *In verbis*: “Art. 63. A competência do Juizado será determinada pelo lugar em que foi praticada a infração penal”.

maior conforto e para que surgisse um crescimento em sua produtividade. O afastamento do contato direto com certas atividades, concentrou esforços em conectar máquinas.

Mas o evoluir da tecnologia trouxe o relacionamento entre pessoas usuárias da informática. A capacidade de conectar-se fez com que o ser humano desenvolvesse, através de computador, ferramentas para socialização e interação com outras pessoas, físicas e jurídicas. Contudo, a socialização feita através da máquina mostrou-se fria. O conversar quase que imediato através de palavras escritas trouxe a sensação de presença, mas trouxe dúvida e equívocos sobre o interlocutor, o que incentivou práticas deturpadas. Diz Emily Finch que:

“Não era de se esperar nada diferente nesse meio ambiente; não só transmite um senso de anonimidade que oferece proteger da detecção os fraudadores, como também liberta indivíduos para agirem de formas descaracterizadas e que não seriam contempladas na vida real.”¹⁴⁸

Por conta de qualquer pessoa poder utilizar a tecnologia, surgiu a insegurança no que se refere ao usuário conectado, que não possui em regra identidade pessoal, mas tão só uma identidade presumida, através da máquina conectada ou de uma conta criada.

A esta identificação presumida feita com base nos dados informados por cada usuário, ou presumida por um número IP de uma máquina, gerou-se o fenômeno da anonimidade.

Por anonimidade virtual, entende-se a falta de certeza quanto à identidade imediata referente a um usuário, levando-se em conta a impossibilidade de se atribuir o uso de um maquinário a uma pessoa.

Existem mecanismos que intentam diminuir as incertezas geradas pela anonimidade virtual como o uso de nomes de usuário associados a senhas (chaves de acesso), o uso de mecanismos de identificação por biometria – leitura palmar, leitura digital, leitura de íris, etc –

¹⁴⁷ NUCCI, Guilherme de Souza. Op. cit. pp. 112-113; ROSSINI, Augusto. Op. cit. pp. 180-181.

¹⁴⁸ “It is little wonder that criminal behavior flourishes in this environment; not only does it convey a sense of anonymity that offers to protect the fraudster from detection, it also frees individuals to act in uncharacteristic ways that they would not contemplate in real life.” FINCH, Emily. Op. cit. p. 40.

, o uso de cartões pessoais com senhas variáveis, *tokens*¹⁴⁹, controles de acesso, dentre outros mecanismos. Ressalte-se, todavia, que os mecanismos visam diminuir incertezas e jamais levar à certeza absoluta quanto à identidade do usuário, prevenindo-se ou mitigando-se as dificuldades e inseguranças.

Enfim, as relações informáticas têm como característica fundamental, por ocorrerem através de aparatos, a falta de certeza absoluta acerca das características do usuário interator, levando a uma dificuldade imediata de identificação do autor dos atos ocorridos.

VELOCIDADE

A última característica de importância fundamental é a velocidade. Uma vez que a cada dia as conexões tornam-se mais velozes, a transferência de dados passa também a ser feita em espaços mais curtos de tempo.

Assim, arquivos maliciosos, por terem tamanho diminuto, terminam por ingressar em aparatos alheios em fração de segundo, de maneira praticamente imperceptível pelo usuário, dificultando sua proteção e domínio dos acontecimentos dentro da máquina.

Outra característica fundamental trazida pela velocidade das conexões e dos processamentos de dados está nos crimes de violação de direitos autorais provenientes de peças audiovisuais, mídias fonográficas e até mesmo programas de computador. Com o advento da velocidade crescente de transferência de dados, mais usuários terminarão por ser incentivados a baixarem um grande número de dados, violando propriedades imateriais dos autores. A velocidade aumenta tanto a possibilidade de baixar (*download*) arquivos legalmente protegidos para as máquinas, quanto carregar na rede (*upload*) peças protegidas. E quanto maior a velocidade e a capacidade de armazenamento, maior a incidência de tais ações violadoras de bem jurídico.

Finalmente, é peculiar à velocidade a maior e mais eficiente navegação pela rede

¹⁴⁹ Entenderemos por *token* o aparelho detentor de uma tecnologia de geração de senhas aleatórias que impedem que um usuário diverso do portador do aparato consiga conhecimento das chaves de acesso necessárias para efetuar operações como ingressar num sistema, perpetrar uma transação bancária, etc.

mundial de computadores elevando a capacidade de ataques (contaminações por *malwares*, escravização de máquinas, etc.) assim permitindo uma maior abrangência nas abordagens como a criação de múltiplos *sites*-armadilha (que contenham *scripts* em suas páginas que terminam por instalar arquivos nas máquinas dos usuarios acessantes), a possibilidade de ataques múltiplos e até a prática de envio de mensagens comerciais não solicitadas em quantidade bastante intensa.

PRINCIPAIS DELITOS INFORMÁTICOS PRÓPRIOS TIPIFICADOS

Os delitos informáticos, sejam próprios ou impróprios, puros ou impuros, envolvem uma multiplicidade de sujeitos envolvidos.

Tome-se como exemplo a conduta de alguém que é contratado pelo presidente de uma indústria automotiva para obter acesso a dados sigilosos presentes nos arquivos eletrônicos de seu concorrente. O cidadão aceita o serviço e acessa os dados a partir de seu conhecimento adquirido em explorar falhas de segurança de sistemas.

A priori, os sujeitos envolvidos no delito são especialmente o autor mediato (pessoa jurídica indústria automotiva) e o autor imediato (*hacker*), além da vítima (pessoa jurídica empresa automotiva invadida). Contudo, é característica do delito informático a multiplicidade de pessoas envolvidas. Suponha-se que para obter o acesso irregular o *hacker* primeiramente dirija-se a uma *LAN house* que, por sua vez, paga a um provedor para obter acesso à rede. Suponha-se que, na sequência, ao invés de o *hacker* explorar uma falha de segurança do sistema, ele opte por enviar um *email* para um funcionário, fingindo-se passar por um cliente e solicitando que este encaminhe ao responsável pelo banco de dados um arquivo anexo. O responsável, então, confiando no funcionário de dentro da empresa, abre o arquivo e acaba por instalar um programa que fica oculto e permite a invasão ao sistema informático. Estariam todos envolvidos no delito informático?

A escolha dos usuarios-alvo depende de variáveis, que na maioria dos casos é fornecida pelas próprias vítimas, em especial nos crimes que exigem interação ou preparo prévio.

Imprescindível, que antes de adentrar na breve exposição dos delitos informáticos, aluda-se à uma classificação bastante utilizada na doutrina européia: a de delitos de relacionamento e delitos de intervenção.¹⁵⁰.

Os primeiros seriam, mas palavras de Schulz, “aqueles feitos que se geraram em uma determinada relação humana ou ao menos foram determinados de modo decisivo por tal relação¹⁵¹”. Seriam condutas em que vítima e vitimário necessariamente estabeleçam confronto direto e atual, e que têm como exemplo principal o estelionato, visto que não há como o delinquente induzir ou manter alguém em erro sem manter contato e interação.

Os delitos de intervenção, em oposição, são aqueles em que o tipo não pressupõe que a vítima participe no comportamento, bastando a ação unilateral do autor¹⁵².

O relacionamento a que nos referimos será explanado com maior afinco adiante, pois que abordaremos a parêntese vitimal e as participações das vítimas no cometimento dos delitos informáticos próprios puros, seja por autocolocação em risco, seja por omissão, seja por ação.

Conforme já explanado, este trabalho busca mostrar a relação entre os crimes informáticos e a importância do estudo da vítima e de sua participação em tais delitos. Dessarte, imprescindível que sejam apontados os principais crimes cometidos com o uso de tecnologia, sejam próprios ou impróprios, para que, na sequência, se possa demonstrar nesses casos como a vítima deve ser analisada. Necessário esclarecer-se, também, que os tipos a seguir apresentados não existem necessariamente no ordenamento jurídico brasileiro. Ainda enfrenta-se a inexistência de uma legislação penal focada nos denominados crimes informáticos próprios puros que em sua essência criaram violações a bens jurídicos antes inexistentes.

Faz-se tal exercício não com ganas de esgotar os crimes informáticos próprios

¹⁵⁰ CARRASCO, Julia Roper. ¿Hay que “Merecer” La Protección Del Derecho Penal?: Derechos y Deberes de Las Víctimas. *La Respuesta Del Derecho Penal ante los Nuevos Retos* (Org. Antonio Cuerda Riezu e Beatriz García Sánchez) Dykinson, 2006, pp. 120-121.

¹⁵¹ SCHULTZ, ZStrR 71 (1956) *apud* MELIÁ, Manuel Cancio. Reflexiones sobre La “Victimodogmatica” em La teoria Del delito. In Revista Brasileira de Ciências Criminais. Ano7, n. 25, janeiro-março de 1999. Instituto Brasileiro de Ciências Criminais, São Paulo, 1999, p.41.

¹⁵² MELIÁ, Manuel Cancio. Reflexiones sobre La “Victimodogmatica” em La teoria Del delito. In Revista Brasileira de Ciências Criminais. Ano7, n. 25, janeiro-março de 1999. Instituto Brasileiro de Ciências Criminais,

existentes nas legislações (alienígenas e brasileira) ou exaurir as explanações necessárias para cada um dos tipos que serão apresentados, mas tão só para que a vitimodogmática, em capítulo posterior, possa ser observada no caso concreto, tendo-se em vista que os comportamentos dos indivíduos mudaram graças à nova sociedade informacional. Para tanto, restringir-se-á a apreensão aos tipos puros.

INTRUSÃO INFORMÁTICA

O tipo aqui denominado refere-se ao ingresso não autorizado¹⁵³ de um usuário no sistema alheio, seja ou não para obter alguma vantagem, seja ou não através de meios ardilosos, violentos, ou até mesmo por conta de um subterfúgio que venha a enganar o legítimo detentor dos direitos relativos ao sistema, levando-o a permitir o ingresso, sob erro.

Inicialmente denominado de invasão informática, o delito foi primeiramente pensado como sendo aquele pelo qual conhecedores de informática atacariam sistemas fechados provocando verdadeiras quebras e aberturas nos mecanismos de defesa (*breakage*), a partir do que obteriam uma via aberta para ingressar nos sistemas alheios.

Uma análise mais detida no modo de atuação dos delinquentes de tais ações, mostra-se diferente: não necessariamente há o uso de mecanismos de violação dos sistemas alheios para a obtenção de acesso.

Em verdade, boa parte dos sistemas operacionais e programas de uso corriqueiro¹⁵⁴ são lançados no mercado com aquilo que se apelidou de *bugs*, que são falhas lógicas de programação. Tais falhas podem gerar brechas de segurança que levam a acessibilidade do sistema e informações alheios por parte de usuários eivados de *dolus malus* e interessados em aproveitarem de tal abertura para quaisquer fins.

São Paulo, 1999, p.41.

¹⁵³ Também é considerada intrusão informática o excesso doloso de acesso autorizado, ou seja, o ingresso autorizado em sistemas limitado a determinadas áreas mas que o delinquente ultrapassa dolosamente. Nesse sentido o Computer Fraud and Abuse Act, 18 U.S.C. §1030. Disponível em <http://www.law.cornell.edu/uscode/18/1030.html>. Acesso em 06.01.09 às 01:46hs.

¹⁵⁴ Navegadores, editores de texto, editores de foto, planilhas, etc.

Também é uma prática bastante comum nas redes informáticas a indução de vítimas futuras e eventuais a instalarem arquivos que geram falhas de segurança ou criam verdadeiras portas de acesso livre nos dispositivos alheios. Uma vez instalados tais códigos maliciosos, o delinquente passa a poder ingressar no sistema.

Diante disso, o termo invasão informática (ou invasão de sistemas) não nos parece o mais adequado. Isso pelo fato de que o substantivo dá a entender um ato violento e até mesmo hostil feito pelo *hacker*, o que não necessariamente é verdade, conforme apresentado¹⁵⁵.

Por vezes, o usuário sequer percebe que seu aparato sofreu uma violação de privacidade, pois que a instalação de um programa faz com que se passe a haver uma verdadeira entrada escondida, de acesso livre e desimpedido, e que é conhecida no jargão informático como porta dos fundos ou *backdoor*. Nenhuma violência terá havido.

É, também, de constatação diária, que boa parte dos usuários, ao serem impelidos a escolherem senhas para acessar suas contas de *email*, sistemas operacionais ou até mesmo *Internet banking* optam por combinações óbvias de símbolos como os números referentes a suas datas comemorativas (de nascimento, de casamento, de nascimento de filhos, etc) primeiros dígitos de números de documentos ou até mesmo seus próprios nomes. Com isso, a probabilidade de alguém interessado ter acesso ao sistema alheio por tentativa e erro e a partir de um pequeno conhecimento pessoal do usuário é de grande êxito.

Outra forma bastante eficaz para se obter as chaves de acesso aos sistemas de usuários é simplesmente pedindo ao detentor dos direitos¹⁵⁶. Assim, também pessoas responsáveis por informações importantes para obtenção de acesso privilegiado em empresas, se corretamente sugestionadas, mostram-se dispostas a cederem dados restritos¹⁵⁷.

¹⁵⁵ Neste sentido, MITNICK, Kevin David. Op. cit., *passim*.

¹⁵⁶ Pesquisa da empresa *Infosecurity Europe*, do Reino Unido, demonstrou que mais de 25% das pessoas que receberam chocolates de um entrevistador mostraram-se dispostas a ceder suas senhas. Disponível em <http://www.globalsecuritymag.com/Survey-by-Infosecurity-Europe,20080416,2687>. Acesso em 05.01.09 às 14:59hs.

¹⁵⁷ MITNIK, Kevin D. e SIMON, William L. O elo mais fraco da segurança in *A Arte de Enganar*. Op. cit, pp. 2-9.

Por isso, prefere-se o termo intrusão que, termo mais amplo, aponta para uma concepção mais abrangente, definida como a ação de se introduzir, sem direito ou por violência, ou, alternativamente, o ingresso ilegal, sem convite.

Qualquer que seja a maneira pela qual o meio de acesso ao sistema informático de um usuário seja obtido o ingresso em bem jurídico (propriedade) alheio exige anuência e permissão, sob pena de ser considerado abusivo.

Não à toa a doutrina chegou a comparar tal conduta com o crime de violação de domicílio, e, em casos em que há superação de contra-senhas ou outro sistema de segurança, com cópias de arquivos, um possível crime de furto com a qualificadora de uso de chave falsa ou o uso de destreza¹⁵⁸.

Certo é que é fato intrusivo pode não gerar qualquer outra atividade senão o desafio da superação dos impedimentos do sistema alheio, sem qualquer prejuízo. Alternativamente pode gerar demais consequências como a modificação de arquivos, a cópia de segredos, a inserção de códigos maliciosos e até a obtenção de numerais particulares de alguém, por parte do delinquente.

A violência da conduta está no fato de que o acesso e tudo o que está relacionado com ele são individuais, exclusivos e somente podem ter seu caráter íntimo e pessoal publicado por quem detém o direito de divulgação e permissão. O ingresso desautorizado, assim, viola a confidencialidade do acesso particular e, conseqüentemente, a segurança telemática, dando incertezas ao usuário violado e levando-o à perda de confiança num instrumento imprescindível para o desenvolver da sociedade.

“FURTO” DE IDENTIDADE

“Furto” de identidade é a apropriação das características e identificações pessoais de outrem para fazer-se passar por este, sem que, contudo, tenha recebido autorização para

¹⁵⁸ LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. Millennium Editora, Campinas, 2006, p. 54-56.

tanto¹⁵⁹. De acordo com a legislação norte americana de 1998 denominada “*Identity Theft and Assumption Deterrence Act*” (Lei de Prevenção a Furto de Identidade ou ITADA), tal conduta poderia ser descrita como aquela em que

*“Intencionalmente alguém transfere ou usa, sem autorização legal, meios de identificação de outrem com a intenção de cometer, auxiliar ou encorajar qualquer atividade ilegal que constitua violação de lei federal, ou que constitua crime de acordo com a legislação”*¹⁶⁰

A anonimidade do ciberespaço faz com que cada usuário conviva e interaja com outros usuários sem nunca ter a certeza de quem são na vida real. Para diminuir esta insegurança, os ambientes de inter-relação terminam por criar sistemas de identificação presumida, em que cada interessado em acessá-los vê-se obrigado a fornecer certos dados, como por exemplo, apelido, nome completo, endereço, numerais de identificação, contra-senha de acesso, endereço válido de *email*, entre tantas outras informações que acabam por compor um delineamento do usuário.

Ao longo do desenvolver da sociedade informacional um indivíduo acaba por criar um perfil virtual imputado¹⁶¹, em boa parte referência de suas características reais, mas não obrigatoriamente¹⁶², uma vez que lastreado em informações cedidas conforme interesse.

¹⁵⁹ Exemplo recente foi o fato de que a polícia de Santa Catarina prendeu um advogado por falsidade ideológica acusado de ter criado perfis na rede social ORKUT fazendo-se passar por um casal, difamando-os quanto à suas personalidades e honra. <http://noticias.uol.com.br/cotidiano/2008/08/14/ult5772u559.jhtm> Acesso em 14.08.08 às 19:32hs

¹⁶⁰ “*Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law*”. A legislação pode ser encontrada em <http://www.ftc.gov/os/statutes/itada/itadact.htm>. Acesso em 14.12.08 às 20:57hs.

Outra definição interessante é de BERG que “*Identity theft is committed by obtaining unique personal information and then using that information to impersonate one or more victims, in one or more locations, across a time period spanning hours to years*”. BERG, Sara E. Identity Theft Causes, Correlates, and Factors: A Content Analysis. In Crimes of the Internet. Pearson Prentice Hall, New Jersey, 2008, p. 225-226.

¹⁶¹ Dizemos que o perfil é imputado por conta de não poder ser considerado legal, visto que a associação pragmática entre o usuário e o indivíduo é relativa. Nesse sentido, FINCH quando apõe que “*This characterisation is more akin to identifiability than identity. Legal identity serves a pragmatic function as its purpose is to create an unbreakable association between a collection of factual information and the individual to whom this relates*”. FINCH, Emily. The problem of stolen identity and the Internet. In Crime Online. Willan Publishing, Devon, 2007, p.31.

¹⁶² É de se ressaltar que a criação do perfil depende de informações fornecidas pelo usuário e que, caso este assim

O uso da rede gera preferências, gera um histórico de locais mais visitados, cria interface personalizada, *habitualidade* na comunicação com amigos ou conhecidos através do meio virtual e assim sucessivamente. Por isso, é possível dizer que uma pessoa tem uma identidade própria no ciberespaço, a partir de seu acesso, e que essa identidade social pode ser de grande valia para sua profissão e relacionamentos¹⁶³. A identidade virtual, então, termina por ser pessoal, mas trata de um conceito de alguém frente a seus núcleos de interesse, de acordo com a similitude.

O tipo em tela trata da ação de um indivíduo que se utiliza da identidade virtual de outro, fazendo-se passar por ele, relacionando-se com as pessoas do convívio alheio, enviando mensagens, utilizando um perfil e aproveitando de sua confiabilidade e preferências, num verdadeiro apoderamento da vida virtual – ou qualquer de seus segmentos – e de seus frutos, que são colhidos por conta do esforço para construí-la¹⁶⁴.

A ilegalidade da conduta está no uso de confidencialidade e credibilidade alheias para proveito próprio – uso ou venda – , à revelia de seu detentor titular, além dos danos patrimoniais e emocionais adjuntos. Exige-se que o uso da personalidade virtual aparente seja feito sem que tenha havido autorização para tanto, porém. A permissão de alguém para remeter uma mensagem em seu nome, ou conversar utilizando-se do apelido de outrem, são exemplos de atitudes que não violam qualquer bem jurídico pois a autorização ilide o caráter furtivo, tendo-se em vista ser a identidade virtual disponível e também, pelo fato de que há pressuposição de dissenso da vítima sob pena de estar-se diante de causa excludente de antijuridicidade na forma de consentimento do ofendido¹⁶⁵.

deseje, será totalmente fantasiosa e distante da realidade. Contudo, grande parte dos usuarios possui um perfil que representa sua realidade e suas características pessoais referidas. A essência do ciberespaço está em permitir que, caso um indivíduo queira, possa pretender ser alguém que não é em verdade para viver situações que não viveria na vida real por falta de coragem, oportunidade, por vergonha ou outro fundamento. Contudo, em regra perfis falsos são criados para atos específicos e, se perdidos, não geram grandes prejuízos para seus legítimos detentores de direitos, fato diametralmente oposto quando se trata de uso indevido de um perfil real, apto a gerar uma gama de dificuldades ao detentor, inclusive na vida real.

¹⁶³ “*As such, the presentation of na appropriate persona is a means of negotiating everyday life and surviving complex social interactions.*” FINCH, Emily. Op. cit., p. 30.

¹⁶⁴ Enquanto que a identidade legal é atribuída no momento do nascimento, com a atribuição de nome, números de identidade, sexo, local de nascimento, etc, a identidade virtual soma a legal com outro segmento maleável e construído de acordo com o interesse de cada usuario.

¹⁶⁵ BITTENCOURT, Cesar Roberto. Tratado de Direito Penal – Volume 3, 3ª Edição. Editora Saraiva, São Paulo, 2006, p. 15

Ao utilizar-se a expressão “furto”, percebe-se uma atecnia. Uma vez que a legislação penal brasileira respeita o Princípio da reserva legal exigindo que todos os elementos normativos estejam presentes para a configuração de um tipo penal, verifica-se que furto em si não há.

O tipo previsto em nosso ordenamento jurídico no artigo 155 do Código Penal apresenta que cometerá ação punível aquele que “*subtrair coisa alheia móvel para si ou para outrem*”.

A identidade é um conceito abstrato, representado por uma quantidade de características e atributos, o que já de início afasta a ideia de que pode ser considerada coisa móvel. Ainda que o ordenamento dê aos bens imateriais como programas de computador, direitos autorais e até energia elétrica a equivalência de proteção dada bens móveis, ainda assim a identidade virtual não se inclui em tais apontamentos por ser em verdade uma legitimidade de acesso a um perfil criado e mantido¹⁶⁶.

Ainda que se acate as propostas legislativas de equiparar dados a coisas¹⁶⁷, ainda que se considere que para o uso da identidade virtual alheia há a necessidade de se possuir os dados existentes no dispositivo alheio, ainda assim o núcleo do tipo não estaria atendido.

Ocorre que por conta dos *bits* que compõe os dados serem intangíveis, e somente representações de uma linguagem a ser interpretada pelo dispositivo, não existe a possibilidade de subtraí-los, mas tão somente de replicá-los (copiá-los) para outro dispositivo, havendo, então, pluralidade de originais idênticos¹⁶⁸.

Não há a possibilidade lógica de se retirar da esfera de vigilância de alguém um dado.

¹⁶⁶ FINCH, Emily. Op. cit., pp. 29-31.

¹⁶⁷ Especialmente o projeto de lei de autoria do deputado Eduardo Azeredo, substitutivo do Projeto de Lei da Câmara (PLC) n° 89, de 2003 (n° 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) n° 137, de 2000, e n° 76, de 2000, que, em seu artigo 3° propõe a criação do artigo 183-A, nos seguintes moldes: “Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.”

¹⁶⁸ É também de se esclarecer que ainda que o arquivo original do dispositivo seja apagado, ainda assim não se pode dizer que ele deixou de existir ou foi destruído, tendo-se em vista que apagar um arquivo é a ação de colocar no início do código de programação o numeral 0 (zero), fazendo com que o aparato informe que o espaço ocupado pelo arquivo – em geral magnético – está disponível para uma futura gravação. Por este motivo que existem formas de recuperar arquivos já apagados e que não se pode falar em retirada de dados ou destruição propriamente dita.

Somado a esta impossibilidade está o fato de que o ordenamento penal brasileiro adota a “teoria da inversão da posse” em que se exige que, para o cometimento do furto, o agente subtraia a coisa móvel e a tenha como posse mansa e tranquila¹⁶⁹.

Por certo tal raciocínio houve no sentido de pressupor-se que o bem tratado e violado é composto por átomos e somente pode pertencer a um único indivíduo e, por isso, a posse seria exclusiva. Contudo, se aplicam tais premissas ao se tratar de dados.

O uso do termo por parte da doutrina dá-se por conta de a expressão predominante da conduta, em língua inglesa ser “*identity theft*” (ou “*identity fraud*”¹⁷⁰). Contudo, ainda que a tradução da expressão seja furto de identidade, ainda assim ela torna-se incompatível com nosso ordenamento jurídico. O motivo é que a definição da palavra “*theft*” está distante da ideia de furto ou roubo porquanto trata de um tomar conta de algo pertencente a outrem, sem seu livre consentimento, sem que este ato recaia sobre um bem jurídico exclusivo, material ou imaterial.

Por sua vez, a legalidade penal brasileira determina que furtos ou roubos somente poderão ocorrer com o ato de subtração, ou seja, partindo da premissa de que o bem jurídico é único – ou de uso único ou pontual, como no caso da energia elétrica –, fato que se distancia da característica plural dos dados informáticos.

¹⁶⁹ Em favor da teoria da concretatio, em que deve haver subtração da coisa e a consumação se dá com a mera retirada da esfera de disponibilidade ou custódia do agente, Edgard de Magalhães Noronha, Damásio de Jesus e Fernando Capez. Em sentido oposto, doutrina majoritária, Luis Regis Prado, Cesar Roberto Bittencourt, Roberto Delmanto, Guilherme de Souza Nucci. A jurisprudência também se divide; exemplo da primeira posição: STJ, REsp 1053764 / RS, 5ª T., 02.09.07, Relator: Ministro Félix Fischer; na segunda posição STJ REsp 810407 / RS, 6ª T., 25.02.08, Relator: Ministro Nilson Naves.

¹⁷⁰ Há certa discussão doutrinária quanto aos termos serem sinônimos. Para alguns, a fraude de identidade (identity fraud) seria a utilização momentânea da identidade de outrem para um propósito específico – uma espécie de furto de identidade de uso –, enquanto que o “furto” de identidade (identity theft) seria a apropriação da identidade alheia com ânimo definitivo, levando o “furtador” a viver uma vida sob a identidade de outrem. Por este raciocínio, o crime em tela seria mais propriamente o de fraude de identidade. Contudo, popularizou-se o termo “furto de identidade”, com o qual ficaremos. FINCH, Emily. Op. cit, p. 34-35. No mesmo sentido, BERG, Sara E. Identity Theft Causes, Correlates, and Factor: A Content Analysis. In Crimes of the Internet. Pearson

INSERÇÃO DE CÓDIGO MALICIOSO

Também denominado inserção de *malware*, contágio de dispositivo alheio ou sabotagem informática, a conduta é da modalidade delitos informáticos próprios puros porquanto a inserção de programas que modificam, alteram ou destroem dados em dispositivos alheios somente pode ocorrer com o uso da telemática.

Isso se dá pelo fato de que códigos maliciosos são instruções inseridas em aparatos alheios que dão comandos que implicam em algum prejuízo, seja na confidencialidade dos dados, seja na disponibilidade (até por perda de velocidade) ou, ainda, na integridade dos mesmos.

Em suma, são programações inseridas que violam o bem jurídico segurança telemática e, com isso, indiretamente podem terminar por causar outros prejuízos.

O Código Penal Japonês, em seu artigo 234.2 tipifica e explica a conduta da sabotagem informática apondo que aquele que insere dados ou dá comandos não autorizado a um computador fazendo-o operar contra seu propósito, está sujeito a pena¹⁷¹.

O Código Penal Alemão em seus artigos 202a, 303a e 303b, com maior abrangência, delinea como sabotagem informática a) a obtenção ilegítima de dados protegidos contra acesso ilegal, para si ou para outrem¹⁷², b) a alteração, supressão, transformação prejudicial ou apagamentos de dados que se dê ilegalmente¹⁷³, e c) a interferência no processamento de

Prentice Hall, New Jersey, 2008, p. 225.

¹⁷¹ Article 234-2. (*Obstruction of Business by Damaging a Computer*) A person who obstructs the business of another by interfering with the operation of a computer utilized for the business of the other or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electromagnetic record used by such computer, by inputting false data or giving unauthorized commands or by any other means, shall be punished by imprisonment with work for not more than 5 years or a fine of not more than 1,000,000 yen. <http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf>

¹⁷² “Section 202a Data Espionage - 1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.” *Strafgesetzbuch, StGB*, traduzido para a língua inglesa e disponível em <http://www.iuscomp.org/gla/statutes/StGB.htm>. Acesso em 06.01.08 às 00:47hs.

¹⁷³ “Section 303a Alteration of Data - (1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (Section 202a subsection (2)), shall be punished with imprisonment for not more than two years or a fine.” *Strafgesetzbuch, StGB*, traduzido para a língua inglesa e disponível em <http://www.iuscomp.org/gla/statutes/StGB.htm>. Acesso em 06.01.08 às 00:47hs.

dados que traga prejuízos substanciais, através da destruição, danificação, inutilização, remoção ou alteração de sistema de processamento de dados ou suporte de dados¹⁷⁴.

Finalmente o Código Penal Italiano, em seu artigo 635 bis, determina que merece intervenção do Estado aquele que destrói, degrada ou inutiliza, no todo ou em parte, sistemas telemáticos alheio, ou programas, dados ou informações alheios¹⁷⁵.

Os danos aludidos nas explicações acima podem ser causados tanto por motivo de ciberterrorismo quanto simplesmente para prejuízo de particular. Certamente no primeiro caso se está diante de crime de ação penal pública, porém, quando o prejuízo ocorrer em âmbito particular, o tipo é o de inserção de código malicioso.

Não se intenta esgotar os possíveis *malwares* nesta explicação, mas somente apresentar exemplos daqueles considerados os mais perniciosos e comuns programas a violarem dispositivos e, mais especialmente, a segurança telemática de alguma forma.

São exemplos deles os vírus, os *rootkits*, os *worms*, os *trojan horses*, os *keyloggers*, os *screenloggers*, os *spywares* e até algumas modalidades de *adwares*, entre tantos¹⁷⁶.

¹⁷⁴ "Section 303b Computer Sabotage - (1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another or a public authority by: 1. committing an act under Section 303a subsection (1); or 2. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be punished with imprisonment for not more than five years or a fine." *Strafgesetzbuch, StGB*, traduzido para a língua inglesa e disponível em <http://www.iuscomp.org/gla/statutes/StGB.htm>. Acesso em 06.01.08 às 00:47hs.

¹⁷⁵ "635 bis *Danneggiamento di sistemi informatici e telematici* - Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni." Disponível em <http://libri.freenfo.net/D/D0000402.html#535>. Acesso em 06.01.09 às 01:13hs.

¹⁷⁶ Os vírus são programas que de regra são criados para se auto-replicarem e serem difundidos automaticamente através dos mais variados suportes. Não necessariamente prejudiciais, sua infecção pode tornar o sistema operacional lento, uma vez que sua grande capacidade de se copiar e espalhar-se pelos principais arquivos faz com que a memória do aparato acabe por ser consumida, tornando lento o processamento dos dados. Podem infectar as máquinas e se multiplicarem imediatamente quando do contágio, podem ser programados para iniciarem sua atividade em dado momento - por exemplo o vírus apelidado "Sexta Feira 13" -, podem iniciar contágio a partir da inicialização do aparato, dentro outras possibilidades. Os *worms* (ou vermes) são muito semelhantes aos vírus, exceto pelo fato de que tem o potencial de contágio aperfeiçoado pois são programados para difundirem-se através da Internet, automaticamente pois acessam os serviços de *email* da máquina, disparando cópias em anexos que chegam à toda a lista de destinatários do usuário infectado. Aproveitando-se da confiabilidade dada às mensagens enviadas pelo usuário hospedeiro, os *emails* contendo os vermes acabam por serem abertos, reiniciando o *modus operandi*, agora na nova máquina contaminada. Os *trojan horses* ou "cavalos

SCAMMING

O verbo “*scam*”, em inglês, representa a ação de defraudar; como substantivo, “*scam*” é um esquema fraudulento de negócios. Tal modalidade de atividade, na rede mundial de computadores, é gênero que abarca diversas espécies menores de condutas prejudiciais. Apenas a título de exemplo, as fraudes perpetradas a partir da rede vão desde o *phishing*, o *pharming*, o estelionato, as fraudes e até mesmo as armadilhas para tomar controle de máquinas alheias. Em resumo, o “*scamming*” é o ato de utilizar-se do meio informático para agir visando obter algum tipo de vantagem sobre o usuário, configurando-se verdadeiro estelionato.

de tróia” são códigos maliciosos com objetivos mais prejudiciais. Inspirados no mito grego, são arquivos com aparência de inofensivos, mas que quando abertos ou executados fazem com que uma programação prejudicial se instale subrepticiamente na máquina infectada, seja com o objetivo de coletar dados como números de cartão de crédito, números pessoais (como CPF, RG, etc) e até mesmo simplesmente dar acesso a um usuário malicioso deixando abertas portas que levam ao controle do dispositivo infectado. *Rootkits* são verdadeiros conjuntos de programas maliciosos que são disparados simultaneamente, cada qual com objetivos específicos. Em regra são um cavalo de tróia que traz junto de si um conjunto de programações que buscam facilitar a camuflagem do arquivo, escondendo os arquivos com técnicas que enganam o sistema operacional. Quando da varredura de arquivos maliciosos por programas de segurança, os rootkits terminam por modificar a forma de pesquisa, por exemplo, levando o programa a não acusar sua existência, dificultando, também, sua remoção, uma vez não sendo acusado. *Keyloggers* e *screenloggers* são arquivos com o mesmo objetivo, mas com mecanismos de funcionamento diferenciados. São programas espões capazes de identificar as ações dos usuários por eles contaminados, e, na sequência, enviar ao usuário mal intencionado tais informações. Assim, os *keyloggers* são capazes de detectar todas as teclas digitadas pelo usuário durante um período de tempo, e remeter ao *email* do *cracker*. Uma vez recebendo o arquivo, o experto visualiza na tela tudo o que foi digitado pelo usuário, inclusive os nomes (*nicknames*) utilizados para acessar programas, contas de *email*, serviços bancários pela Internet e assim sucessivamente, levando a um possível uso indevido de tais dados, trazendo prejuízos na confidencialidade e disponibilidade dos serviços, além de prejuízos econômicos em regra. Após a criação de tais programas maliciosos, os bancos substituíram a digitação de senhas para acesso aos serviços bancário por “teclados virtuais”. Com isso, seus correntistas não digitariam na tela as senhas de segurança, evitando que *keyloggers* instalados pudessem monitorar tais serviços e causarem prejuízos. Contudo, os programadores desenvolveram os *screenloggers*, programas capazes de capturar as telas visualizadas no ciberespaço e o movimento do mouse e ações de clique dos usuários. Com isso, passaram a serem capazes de descobrir as senhas apesar de estas não serem mais digitadas no teclado alfanumérico tradicional. Os *spywares* e *adwares* também têm mecanismos semelhantes de atuação, contudo com objetivos teoricamente diferenciados. Têm ação muito semelhante com a dos *cookies*, que são programas que interagem com os programas de navegação pela rede para guardar as preferências dos usuários e facilitar a navegação por *sites* de acordo com o gosto ou para melhor facilitação no carregamento de arquivos multimídia, num intuito de beneficiar e tornar os ambientes virtuais mais amigáveis. Os *spywares*, são, também, programas automáticos de coleta de ações dos usuários, como seus costumes no ciberespaço; todavia, estes programas espões podem ser programados para encontrarem e guardarem dados confidenciais dos usuários - por exemplo, os logins bancários -, remetendo, então, para seu programador que terá a oportunidade de causar prejuízos diversos, desde estelionatos, até “furtos de identidade”. Os *adwares*, por sua vez, são modalidades de *spyware*, mas com objetivos especiais: exibem automaticamente na tela do usuário contaminado propagandas, geralmente conforme sua preferência ou aquisição de produtos na rede, portanto personalizadas. Em regra, tanto *spywares* quanto *adwares* são programas embutidos em outros programas de distribuição livre e gratuita, não raro sendo legal sua distribuição, uma vez aceita pelo usuário.

Em regra são golpes ou armadilhas (*honey pots* para usuarios bem intencionados) elaborados para que os usuarios menos preparados acabem por agir de acordo com o intuito do delinquente, na rede mundial de computadores.

Também conhecido como “*confidence trick*” ou truque de confiança, é delito de relacionamento em que o ofensor e o ofendido comunicam-se direta ou indiretamente, sendo que o primeiro tenta persuadir o segundo a alguma ação, geralmente a cessão de informações sensíveis ou a transferência de valores em pecúnia ou crédito. Tais ações, quando operadas no ciberespaço, receberam o nome de engenharia social (ou engenhosidade social), sendo tal meio verdadeiro laboratório para os usuarios com *dolus malus* experimentem diferentes técnicas ardilosas para obtenção de valores.

Ações que buscam explorar as vulnerabilidades humanas na rede, sejam positivas, sejam negativas, costumam ser veiculadas em forma de *emails* com histórias ou *sites* com atrativos de manipulação com a expressão “clique aqui”. São classificadas por em diversas categorias¹⁷⁷:

- 1- Esquemas de enriquecimento rápido ou “*Get-rich-quick schemes*” – em que alguém oferece soluções que levariam o usuario a receber rapidamente altas quantias de dinheiro¹⁷⁸;
- 2- Esquemas envolvendo o desenvolvimento de relacionamento mais duradouro –

¹⁷⁷ Como os sites “Monitor das Fraudes” (<http://fraudes.org/>), Consumer Fraud Reporting (<http://www.consumerfraudreporting.org/websitescams.php>) Fraud.org (<http://www.fraud.org/>), Internet Fraud Complaint Center (<http://www.ic3.gov/default.aspx>), dentre outros.

No mesmo sentido, WENDY CUKIER, Avner Levin. Internet Fraud and Cyber Crime. In Crimes of the Internet. Pearson Prentice Hall, New Jersey, 2008, pp. 251-262.

¹⁷⁸ Um dos principais exemplos é o denominado “*nigerian scam*”, hoje também virtual, mas que tem diversas variáveis informáticas como o envio de mensagens por celular (SMS) informando ter havido um sorteio e o ganho de um prêmio exigir um depósito ou o pagamento de uma taxa; também, *sites* com banners com dizeres em que o usuario foi o milionésimo visitante, e que deve seguir um procedimento de concessão de informações privilegiadas ou pagamento de algum valor.

O *Nigerian Scam* (*Advance Fee Fraud* ou *419 Fraud*) é um esquema em que se oferece um emprego de alto escalão na Nigéria, mas que, para isso, exige-se uma série de procedimentos para obtenção de “documentação apropriada”, aluguel de imóveis, pagamento de visto, pagamento de taxas e assim por diante. A isca é o alto salário oferecido e a confiança vai sendo obtida a partir de uma extensa troca de emails e cartas com documentação aparentemente confiável da empresa contratante. Ao final, a vítima termina por transferir uma certa quantia de dinheiro para o vitimário sem que o emprego jamais tenha existido. Tal golpe, muito antigo, iniciou-se através de cartas e hoje difunde-se pelo correio eletrônico com diversas variáveis como o “golpe do fundo esquecido” em que uma mensagem é enviada informando que um parente distante faleceu sem deixar herdeiros e que o vitimário oferece-se para auxiliar a levantar o valor por uma quantidade de dinheiro em troca, dentre outros. <http://fraudes.org/showpage1.asp?pg=45>. Acesso em 29.09.08 às 12:39hs.

geralmente associados a salas de bate-papo, *sites* de relacionamento, *sites* de busca de noivas entre outros, são técnicas utilizadas para seduzir usuarios interessados em encontrar companhia, buscando-se adquirir sua confiança e, assim, obter dados que permitam desvios de recursos, em regra.

Também, há modalidades de serviços em que usuarios são ludibriados para pagarem mensalidades a título de contratação de pretensos serviços de busca de noivas (e troca de mensagens com pretendentes) ou bebês para adoção, sem que jamais obtenham êxito na empreitada.

3- Esquemas que envolvem produtos falsamente valiosos ou *Gold-brick schemes* – trata-se de ação com duplo caráter lesivo. Alguém oferece um produto com uma qualidade prometida, mas após o pagamento e entrega, o material mostra-se falso¹⁷⁹.

Na rede mundial de computadores, os produtos oferecidos podem variar bastante e são, em regra, vendidos em *sites* de leilões por preços muito abaixo do mercado. Os produtos vendidos revelam-se ou falsos, ou de qualidade inferior à prometida, jamais são entregues ou, ainda, são produtos frutos de outra conduta ilícita como furtos, roubos ou apropriações indébitas.

Há também as vendas de drogas ilícitas através da rede, o tráfico de bebês, e, com enorme intensidade, há a modalidade de esquema em que *sites* com conteúdo pornográfico, por seu potencial atrativo advindo de oferecimento de fotos e vídeos sobre o tema, são utilizados como iscas a usuarios que, na busca de satisfazer desejos, clicam em *links* para acessarem material multimídia ou fornecem dados pessoais que terminam por permitir que o ofensor possa proceder a condutas prejudiciais, na sequência, obtendo dados íntimos que permitem práticas futuras de extorsão, uso indevido de identidade, entre tantas outras.

4- Esquemas envolvendo extorsão – são situações em que o delinquente, em posse de informações verdadeiras ou não, exige dinheiro do usuario-alvo para, *p. ex.*, não levar a público uma situação de exposição como preferências sexuais escondidas, relações

¹⁷⁹ Por isso o nome *gold-brick* que significa barra de ouro: alguém oferece uma barra de ouro por um preço bem abaixo do mercado e, após a compra, o adquirente percebe que a barra era somente folhada a ouro, revelando-se, o negócio, enganoso.).

extraconjugais e até mesmo conhecimento de transações bancárias ilegais cometidas por meios informáticos¹⁸⁰.

5- Esquemas envolvendo jogatina – os delitos envolvendo jogos de azar têm tipos próprios; ocorre que há jogos legalizados (ou locais em que a jogatina não é conduta típica) mas que ainda assim são formulados para que o usuário perca dinheiro. Assim, deixam de ser jogos de sorte para ser verdadeiras armadilhas que exploram o vício em jogos dos usuários, a partir de manipulação artificial de resultados, maquiando os resultados dos jogos, sempre levando à perda de dinheiro¹⁸¹.

6- Outros esquemas fraudulentos – a) o principal exemplo de *scamming* por meio virtual, além dos supra apresentados é o *phishing* (ou *phishing scam*) que consiste, nada mais, do que a ação de um vitimário que se faz passar por representante de pessoa jurídica, igreja, ONG ou até mesmo entidades governamentais para conseguir a confiança da vítima e, na sequência, obter dados importantes para uma futura utilização – até mesmo para *identity theft*.

Os principais golpes no momento são os que envolvem a) a alegação de que um documento do usuário foi cancelado (geralmente CPF ou título de eleitor) e que ele deve informar uma ampla quantidade de dados e números pessoais; b) mensagens informando que o usuário deve pagar um boleto anexado para limpar seu nome, tendo-se em vista que está constante na lista de maus pagadores; c) com altíssima incidência, *emails* de bancos em que o usuário é remetido, ao clicar na mensagem, a *sites* espelho, idênticos aos verdadeiros mas fraudulentos e hospedados em servidores fora do país, em que se solicita dados do cartão de crédito, senhas, números de segurança, etc. para que possam haver saques, pagamentos e transferência; d) o envio de mensagens sentimentais que buscam tocar os leitores de um

¹⁸⁰ Também, tem ocorrido na modalidade de sequestro de dados (*data hijacking*), em que o ofensor consegue acesso a arquivos que representam documentos importantes de um usuário e cria longas senhas para prejuízo da vítima que, necessitando do arquivo ou pasta, termina por ceder somas de dinheiro (ou créditos de celular pré-pago, créditos em moeda virtual, etc) em troca da disponibilidade dos dados.

¹⁸¹ O usuário acredita que tem chances verdadeiras de obter resultado positivo e os jogos (no caso, os jogos virtuais) em verdade estão programados para jamais permitirem que o apostador consiga valores altos em suas apostas. Ainda assim, o vício impede o usuário de afastar-se das apostas, mesmo pela rede mundial de computadores. Nesse sentido: GEIS, Gilbert et al. Internet Gambling. *In Crimes of the Internet*. Pearson Prentice Hall, New Jersey, 2008, pp. 166-189; WANG, Chee Keng John. Passion and Intrinsic Motivation in Digital Gaming. *CYBERPSYCHOLOGY & BEHAVIOR*, V. 11, N. 1, 2008, pp. 45. Disponível no site: <http://www.liebertonline.com/doi/pdfplus/10.1089/cpb.2007.0019>. Acesso em 06.01.09 às 01:54hs.

problema aparentemente real – inclusive com fotografias – como, por exemplo, uma criança que precisa de algum transplante, jovens que precisam de contribuições para continuar seus estudos e até mesmo falsas ONGs e falsas igrejas solicitando contribuições.

O capítulo sobre as características marcantes das vítimas tratará mais sobre o temário do *scamming*, demonstrando de que modo os vítimas agem e como são feitas as escolhas de vítimas no meio informático.

SPAMMING

"Spam" seria a nomenclatura popular para o apelido dado às tais mensagens com cunho comercial que infestam as caixas de entrada dos programas de *email* e que, tecnicamente são denominadas UCM ou "*unsolicited comercial messages*" ou envio de mensagens comerciais não solicitadas¹⁸². No campo penal, há bastante discussão doutrinária acerca da relevância da conduta apelidada de *spamming*; uma vez tipificado, o delito poderia ser classificado na modalidade próprio ou impróprio, dependendo da linha adotada. Sendo qualificado como delito próprio, será enquadrado na espécie pura ou direta, conforme exposto abaixo.

¹⁸² No Estado de São Paulo, a Lei Estadual no. 13.226/08 criou o Cadastro para Bloqueio do Recebimento de Ligações de Telemarketing no Estado, que, utilizando-se do sistema opt-out, dá ao cidadão que recebe ligações de telemarketing e semelhantes o direito de entrar em contato com o Procon e registrar sua opção de cessação do incômodo quanto àquela pessoa jurídica, gerando presunção de que novo incômodo poderia gerar algum tipo de sanção.

"LEI Nº 13.226, DE 7 DE OUTUBRO DE 2008 (Projeto de lei nº 478/08, do Deputado Jorge Caruso - PMDB) Institui no âmbito do Estado de São Paulo, o Cadastro para o Bloqueio do Recebimento de Ligações de Telemarketing. O GOVERNADOR DO ESTADO DE SÃO PAULO: Faço saber que a Assembléia Legislativa decreta e eu promulgo a seguinte lei: Artigo 1º - Fica instituído, no âmbito do Estado de São Paulo, o Cadastro para o Bloqueio do Recebimento de Ligações de Telemarketing. Parágrafo único - O Cadastro tem por objetivo impedir que as empresas de telemarketing, ou estabelecimentos que se utilizem deste serviço, efetuem ligações telefônicas não autorizadas para os usuários nele inscritos. Artigo 2º - vetado. Artigo 3º - vetado. Parágrafo único - vetado. Artigo 4º - vetado: I - vetado; II - vetado; III - vetado; IV - vetado; V - vetado; VI - vetado; VII - vetado. Artigo 5º - A partir do 30º (trigésimo) dia do ingresso do usuário no Cadastro, as empresas que prestam serviços relacionados ao parágrafo único do artigo 1º ou pessoas físicas contratadas com tal propósito, não poderão efetuar ligações telefônicas destinadas às pessoas inscritas no cadastro supracriado. § 1º - vetado. §2º - Incluem-se nas disposições desta lei os telefones fixos e os aparelhos de telefonia móvel em geral. §3º - A qualquer momento o usuário poderá solicitar a sua exclusão do Cadastro. §4º - vetado. §5º - vetado. Artigo 6º - Não se aplicam os dispositivos da presente lei às entidades filantrópicas que utilizem telemarketing para angariar recursos próprios. Artigo 7º - Esta lei entra em vigor na data de sua publicação. Palácio dos Bandeirantes, 7 de outubro de 2008. Publicada na Assessoria Técnico-Legislativa, aos 7/10 de 2008."

Contudo, é de se ressaltar que não são somente as mensagens comerciais que assoberbam a vida dos usuarios, tomando-lhes tempo para leitura e descarte. Parte do denominado "lixo virtual" ou "lixo eletrônico" é composta por UPM – “*unsolicited pornographic messages*” - ou mensagens pornográficas não solicitadas e, em determinados momentos - normalmente em biênios -, no Brasil, UEM - “*unsolicited electoral messages*” - ou mensagem com conteúdo de propaganda eleitoral não solicitadas também passam a ser grandes embaraços e exigem esforço dos usuarios para bloqueio e eliminação¹⁸³.

Seus usos vão desde marketing legítimo até veículo para perpetração de fraudes, apropriação de identidades e disseminação de vírus. Afora a possibilidade de mensagens com cuinhos duvidosos serem portas de entrada para diversos fins e meios de explorar a ignorância do usuario, nesta etapa tratara-se das mensagens sem qualquer outro objetivo que não o de propagandear ideias ou publicizar produtos.

Diversos países já legislaram acerca da matéria, como por exemplo os Estados Unidos da America do Norte - *CAN-Spam Act* - a Australia - *Spam Act* - a União Européia - *Directive on Privacy and Electronic Communications* - a Nova Zelândia, - *Unsolicited Electronic Messages Act 2007* - o Canadá, - *Personal Information Protection and Electronic Documents Act* - Singapura, - *Spam Control Act 2007* - Hong Kong, - *Unsolicited Electronic Messaging Ordinance* - a China, - *Regulations on Internet E-Mail Services* - a Malasia, - *Communications and Multimedia Act 1998* - Israel, - *Protection of Privacy Law 5741-1981* - *The Law on Regulation of Transmission of Specified Electronic Mail* - e Argentina – *Ley de Proteccion de los Datos Personales* –, dentre outros. Porém, sua criminalização ainda não é frequente.

O que se nota é que a maioria das legislações determina a forma como o *spam* pode ser enviado para usuarios sem que a conduta seja considerada irregular. Há uma nítida divergência entre legislações: predominantemente na Europa, determinou-se que a conduta de envio de mensagens não solicitadas exige uma manifestação positiva do destinatário para poder

¹⁸³ Aqui vale um paralelo. Afora os *spams* que ingressam nas caixas de correios dos usuarios, outras mensagens não solicitadas também incomodam: as chamadas telas *pop-up* que atrapalham a navegação do usuario e poluem visualmente o meio ambiente informático de modo a reduzir dinâmica da rede. Na França, o spam é denominado “pollurriel”, um neologismo relacionado à palavra “*pollu*” que significa “poluição”. ZANELATO, Marco Antonio. Condutas Ilícitas na Sociedade Digital. In *Direito e Internet*. Ano II, n. IV – Julho de 2002. Escola Superior do Ministério Público de São Paulo, São Paulo, 2002, p.194.

acontecer. Nos Estados Unidos da América do Norte e Japão a conduta de remessa de mensagens é inicialmente permitida, até que o usuário alvo determine o fim das remessas¹⁸⁴.

Ao primeiro sistema apresentado, denominou-se OPT-IN, pois que o *email* de cada usuário somente pode fazer parte do banco de dados dos *spammers* se e somente se houver a manifestação de aceitação de tais recebimentos, ou seja, opção para ingresso na lista de destinatários. Tal anuência de dá no clique na caixa de diálogo contendo dizeres como "eu quero receber mensagens informando sobre produtos", "eu desejo receber *emails* com novidades da empresa X" ou até mesmo selecionando as áreas de interesse para o recebimento de ofertas, propostas ou afins. O envio de mensagens sem autorização expressa, então, levaria à condição de ilegalidade de conduta, podendo o remetente inclusive ser punido criminalmente.

O segundo sistema apresentado recebeu, inversamente, a nomenclatura de OPT-OUT. Inversamente ao explanado acima, é um sistema em que há liberdade inicial para envio de mensagens aos usuários, que, em não desejando mais recebê-las faz um movimento positivo de saída, requerendo que seu endereço eletrônico seja retirado do banco de dados que remete as mensagens aludidas. Enquanto que no primeiro sistema o usuário pede - ou aceita - entrar (opta pelo ingresso, ou "*option in*"), neste segundo, o usuário pede para sair (opta pela saída, ou "*option out*")¹⁸⁵.

O Brasil ainda não se posicionou formalmente acerca do sistema a ser adotado. Contudo, houve tendência pelo segundo sistema, semelhante ao norte-americano, até recentemente, com projeto em tramitação no Senado Federal, de autoria do senador Delcídio do Amaral (PT-MS) que, em contrapartida, propôs a adoção do sistema europeu¹⁸⁶.

¹⁸⁴ Informações disponíveis em <http://www.spamlaws.com/world.shtml>. Acesso em 09.01.09 às 18:53hs.

¹⁸⁵ ZANELATO, Marco Antonio. Op. cit. pp. 201-204.

¹⁸⁶ Duas decisões de especial interesse quanto ao tema, ainda que em sede cível, ambas de juízos do Rio Grande do Sul e que merecem transcrição de ementa, pois que focadas no tema: Apelação Cível nº 71001280536/2007 ("OBRIGAÇÃO DE NÃO FAZER. ENVIO DE E-MAILS. SPAM. A sentença recorrida é clara e se atém aos limites do pedido, ou seja, que a parte demandada se abstenha de remeter ao autor os chamados "spam" que são mensagens eletrônicas não solicitadas, quase sempre com o cunho publicitário. SENTENÇA MANTIDA. RECURSO DESPROVIDO.") e Agravo de Instrumento nº 70025172263/2008 ("AGRAVO DE INSTRUMENTO. AÇÃO CAUTELAR INOMINADA. RESTABELECIMENTO DA PRESTAÇÃO DE SERVIÇO. ENVIO DE SPAM'S. NECESSIDADE DE DILAÇÃO PROBATÓRIA. A partir das alegações das partes, uma sustentando tratar-se de envio de spam's, atividade reconhecidamente ilícita, outra, que se trata de envio de e-mail's

É interessante que se compreenda o porquê de se taxar tais remetimentos como conduta ilícita e que enseje movimento penal do Estado.

Três são as linhas argumentativas apresentadas pela doutrina. A primeira segue a ideia de que o envio de mensagens não solicitadas é verdadeira perturbação do sossego alheio pois que ninguém é obrigado a ser importunado com mensagens de cunho erótico, político ou comercial sem expressamente anuir com tal conduta. A partir disso, o email seria somente uma das ferramentas possíveis para obter a violação da paz pública, sendo a conduta mero delito informático impróprio pois o ferramental tecnológico seria um somente eleito dentre diversos possíveis.

A segunda linha parte do pressuposto de que o envio de tais mensagens, sejam elas encaminhadas para a caixa de entrada da caixa de correio eletrônico, sejam encaminhadas para a lixeira, gera um dispêndio de tempo por parte do destinatário. Isso porque os sistemas de filtragem de conteúdo ainda não apresentam total confiabilidade, fazendo com que, por vezes, mensagens importantes vão parar em pastas incorretas. Cabe ao titular da conta, certamente, a administração das mensagens que recebe, o que faz com que sistematicamente seja necessário o esvaziamento da lixeira da caixa de *emails* além da usual leitura das mensagens recebidas. O fato de se receber um grande número de mensagens não solicitadas acaba por gerar diariamente uma perda de tempo (segundos, minutos) mas que, pelo Princípio da cumulatividade e ao longo de meses, acaba por representar horas de trabalho perdidas, gerando significativa perda patrimonial, seja para o profissional liberal, seja para a empresa contratante de funcionários, cabendo, pois, responsabilização. Nesse caso o delito seria próprio, porque a única forma de se proceder a tal modalidade de “furto de tempo” seria através de ações informáticas. Porém, o bem jurídico atingido não seria informático, mas sim o patrimônio, atingido indiretamente. Seria, desta forma, delito próprio impuro.

A terceira, por sua vez, considera o envio crescente das mensagens como violação da disponibilidade tendo-se em vista o fato de que gera um congestionamento da rede, em especial dos servidores de *email* prejudicando na velocidade e gerando um custo geral para os

marketing, atividade lícita, revela-se imperiosa a dilação probatória, o que será realizado nos autos da ação principal, com o intuito de se apurar, de forma efetiva, qual argumentação deve prevalecer. Manutenção da decisão agravada. NEGARAM PROVIMENTO AO AGRAVO DE INSTRUMENTO. UNÂNIME.”)

usuários¹⁸⁷. Nesse caso, a única forma de violar o bem jurídico informático disponibilidade seria através de uma conduta que se utilizasse de meios tecnológicos. Assim, o delito seria próprio e da modalidade puro.

INTERCEPTAÇÃO DE *EMAIL*

Tal delito seria representado pela conduta de se impedir que a mensagem de correio eletrônico, enviada por um remetente, atinja seu destinatário. Classificado como crime informático próprio puro por atingir bem informático e por somente poder ser cometida utilizando-se de meios informáticos, pode ocorrer por dois motivos principalmente: pelo fato de que as mensagens são normalmente enviadas sem mecanismos de proteção e pelo fato de que não há mecanismos/autoridades intermediadores que garantam a chegada correta das mensagens a seus destinos.

A mensagem enviada por um programa de envio de correio eletrônico tem um funcionamento bastante simples. Alguém digita em seu dispositivo telemático uma mensagem e especifica um endereço destino representado pelo usuário, o símbolo da arroba e o provedor do serviço destinatário. Este conteúdo é constituído por *bits* que são encaminhados ao provedor remetente do serviço, que, por sua vez, conhecendo o provedor destino, o encaminha, através da rede mundial de computadores.

Ocorre que, conforme já doravante explanado, o remetimento de pacotes de dados contendo o conteúdo da mensagem é feito de maneira livre, ou seja, o tráfego ocorre através dos canais de comunicação da rede, sendo constantemente sujeitos a interceptação por alguém com aparato capaz de captar tais¹⁸⁸.

Para a devida compreensão do dito delito, algumas considerações acerca do vocábulo interceptar diante da realidade informática são necessários.

Interceptar significa colocar-se entre, na qualidade de obstáculo, ou seja, impedir que o

¹⁸⁷ Conforme Roque Abdo, em reportagem *Administrar e-mail fica cada vez mais difícil – spam torna-se grande problema na Web, mas cada provedor tem uma política diferente*, jornal O Estado de S. Paulo, 13.11.2000, Informática *apud* ZANELATO, Marco Antonio, Op. cit. p. 196.

curso dos dados se desenvolva, de modo a impedir que o destinatário obtenha acesso a eles. Ocorre que a rede fraciona os dados em pacotes, que vão sendo remetidos quantas vezes forem necessárias até que o destino seja atingido, de modo a todos os pacotes serem recebidos e devidamente organizados, com capacidade de conversão na ponta destinatária.

Ora, sendo assim, a mera leitura dos dados referentes a um *email* por um terceiro pode não impedir que o destinatário também receba a informação numa posterior remessa de pacotes de dados, portanto, fazendo com que a mensagem atinja seu destino perfeitamente. Isso leva ao afastamento da figura do artigo 10 da Lei no. 9.296/96¹⁸⁹ que aponta o tipo preenchido somente quando a interceptação impedir que a mensagem atinja o destinatário¹⁹⁰.

Por este aspecto especial da informática, Ronaldo Lemos da Direito-GV-RJ compara o *email* a um cartão-postal e não a uma correspondência fechada, levando a uma visão diferenciada da remessa de mensagens, pois que o carteiro, ao ler o conteúdo de um cartão postal não viola correspondência alheia.

Some-se tal raciocínio à leitura do art. 47 da Lei no. 6.538/78 que dispõe sobre os serviços postais no país e ver-se-á que nenhuma das definições traz sequer alusão ao *email* como assemelhado a serviço postal, e estar-se-á diante de uma atecnicidade ao se equiparar a ideia de que a leitura de mensagens eletrônicas configuraria a figura do artigo 151 do Código Penal (Violação de Correspondência)¹⁹¹.

Finalmente, é de se compreender que existem mecanismos de proteção ao sigilo do correio eletrônico como a criptografia, o uso de autoridades certificadoras intermediárias, e até mesmo mecanismos de ocultação de conteúdos sigilosos como a esteganografia.

¹⁸⁸ ALBUQUERQUE, Roberto Chacon de. Op. cit., p. 96 e ss.

¹⁸⁹ "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados"

¹⁹⁰ ROSSINI, Augusto. Op. cit. p. 215.

¹⁹¹ *Ibidem*, pp. 211. O autor, porém, propõe mudança no projeto de lei nº 84/99 acrescentando-se um parágrafo quinto ao artigo 150, com os seguintes dizeres: "Para todos os fins deste artigo, o correio eletrônico (e-mail) equipara-se à correspondência fechada." *Ibidem*, pp. 240-241

A CRIMINOLOGIA E A DIFÍCIL PREVENÇÃO DO DELINQUENTE INFORMÁTICO

De acordo com Pablos de Molina, o estudo criminológico aponta três como sendo as formas de prevenção de conflitos para qualquer espécie de infração penal, compondo prevenção “primária”, “secundária” e “terciária”, levando-se em conta o critério etiológico¹⁹².

A prevenção “primária” é aquela em que se busca combater a cogitação delitiva fazendo-se investimentos em educação, emprego, assistência social, previdência, e que assim afetam a raiz social do conflito criminal, buscando evitar que ele venha sequer a se manifestar¹⁹³.

É natural que a falta de direitos básicos e de condições mínimas de sobrevivência são pavios que levam um cidadão excluído social a cometer delitos. Diante de uma análise comparativa simples, países com menos oportunidades e com maiores desigualdades são, via de regra, mais violentos e com maior índice de criminalidade.

Assim, a intervenção preventiva estatal deve focar as diferenças sociais como gênese do delito, investindo nos setores culturais, econômicos e sociais por períodos longos, criando e evoluindo um novo segmento social mais igualitário e consciente, em que os delitos deixam de ser ponderados como opção, focando-se na produção.

A prevenção “secundária”, por sua vez, atua com foco na experiência obtida a partir da análise empírica da criminalidade, após conhecer-se o tempo e o espaço em que os delitos se exteriorizam com certa frequência.

¹⁹²PABLOS DE MOLINA, Antonio Garcia. Criminologia. 5ª Edição revista e atualizada. Editora Revista dos Tribunais, São Paulo, 2006, pp.312-314.

¹⁹³ Nesse aspecto, cabe citar os dois grandes dilemas do homem, apresentados pelo professor Alvino Augusto de Sá que apresenta em seu livro Criminologia Clínica e Psicologia Criminal, *in verbis*: “O homem, principalmente o homem moderno, o homem do mundo globalizado, vive dois grandes dilemas. O dilema da necessidade premente de vencer, sem pré vencer e ultrapassar os limites do humano (que leva à hubris, a maior das violências perante si e os demais humanos) ou ajustar-se às condições humanas de sobrevivência. É o dilema de vencer as interdições que impedem o indivíduo de se realizar como homem (o que pode levar a conflitos com a lei) ou submeter-se e resignar-se. A minoria dominante vive mais explicitamente o primeiro dilema, o da necessidade premente de vencer, vencer, vencer sempre mais os seus iguais e os que lhe superam em poder e capital, numa corrida desenfreada e louca a procura de ultrapassar os limites humanos e atingir os umbrais do divino, cometendo, assim a maior das violências, para a mitologia grega, a hubris, que consiste em querer tornar-se o todo poderoso (Bergeret, 1990).”

Embasado no conhecimento pragmático e estatístico¹⁹⁴, o Estado tem, pois, condições de prevenir o acontecimento da infração penal agindo desde geograficamente (aumentando a iluminação, diminuindo o tempo em que os semáforos ficarão vermelhos, mantendo carros de polícia em cruzamentos, *et cetera*) até através de políticas legislativas, políticas policiais de patrulhamento, e outras.

Tais atos produzem efeitos em prazos médios e curtos, vez que retiram o ambiente propício do delinquente, agindo no foco potencial da ação, desincentivando o atuar naquele local¹⁹⁵. Deve-se considerar, entretanto, que o criminoso planejador de suas ações buscará ambientes mais propícios para o cometimento do tipo caso esteja determinado. Diante de tal fato, é de se compreender que a prevenção “secundária” é paliativa e tem um efeito de prorrogação do momento e região do delito somente.

Finalmente a prevenção “terciária”, que representa um foco de ação estatal diferenciada. Enquanto que as prevenções anteriormente explanadas trazem atitudes focadas em todos os cidadãos genericamente, esta modalidade foca na figura do recluso condenado e na evitação de reincidências.

A intervenção tardia visa utilizar-se de programas “ressocializadores”, “reeducativos” e de reinclusão social, visando dar ao preso condições de, ao sair do estabelecimento prisional, ser capaz de enfrentar o desafio da realocação social sem ser apartado da produtividade e, assim, sem ser incentivado a cometer novos fatos delituosos.

Contudo, o estudo da prevenção apresentado trata de crimes denominados “reais” e que, para que se pudesse ser desenvolvidas tais estratégias, foi necessário o apontamento de traços similares de tal esfera de criminalidade. As já apontadas características, então foram a de que o crime comum exige a) proximidade; b) escala; c) constrangimento físico e d)

¹⁹⁴ Não é errado dizer que a prevenção secundária guarda uma relação interessante com a Escola de Chicago como teoria criminológica, especialmente à ideia de que, a partir do empirismo estatístico e geográfico, das cifras que apontam para o território em que a incidência criminal é maior e em que locais crimes específicos ocorrem com maior intensidade, poderiam as políticas criminais de prevenção secundária ser estabelecidas.

¹⁹⁵ “One is that only a small segment of a functioning society’s populace will persistently engage the criminal activity; those who fall into this category are apt to be from economically deprived backgrounds and reside in areas that share geographic and demographic characteristics. They will be inclined to focus their efforts on those with whom they share a level of physical proximity because they are convenient victims; consequently, much of a society’s routine crime will be concentrated in identifiable areas.” BRENNER, Susan W. *Cybercrime:re-thinking*

padrões¹⁹⁶. Crimes reais são, respectivamente, a) cometidos com a presença física entre ofensor e ofendido, b) crimes em que a ação em regra se dá na modalidade um contra um, ou seja, o contato do ofensor é direto com cada vítima, c) exige o uso de força, presença e planejamento por parte do ofensor, que se expõe e se arrisca, e d) desenvolvem-se de acordo com uma lógica, vestindo-se de generalidades e estilos na prática¹⁹⁷.

Assim, a maior parte das estratégias de contenção forma-se a partir de investimentos públicos em delitos com limitações espaciais, escopo restrito, investigação focada e vítimas limitadas.

Ocorre que quando se trata de delito informático, o problema reside especialmente no fato de que a prevenção primária mostra-se ineficaz, as características especiais tornam inócuas as ações de prevenção secundária e a prevenção terciária somente tem razão de existir num novo conceito de ressocialização.

O delito informático obviamente dispensa a presença física do ofensor, dispensa contatos diretos com a vítima, planejamento e força, ocorrem a partir de uma ação contra uma multiplicidade de pessoas (crimes de um contra muitos) e não respeitam lógica e estilo¹⁹⁸, sendo pois alvo de constantes modificações em suas táticas e ardis. Com isso, é imprescindível entender que a nova criminalidade tenderá a somar-se com a clássica, gerando uma sobrecarga de ações criminais.

Também, as pistas deixadas pelos ofensores virtuais demoram a ser buscadas, encontradas, e ainda assim dependem de fatores que podem tornar sua investigação inócua, como por exemplo o fato de que um desvio de recursos pode se dar instantaneamente para paraísos fiscais de difícil controle legal e ausência de normativos repressores.

Outro item importante é o fato de que normalmente só se nota o crime informático após seu cometimento, o que permite ao delinquente que até mesmo apague as pistas sobre sua ação e paradeiro real; é a prova volátil, temporária e de difícil obtenção.

crime control strategies. Crime Online. Willan Publishing, Devon, 2007, p. 15.

¹⁹⁶ BRENNER, Susan W. Op. cit. p. 14.

¹⁹⁷ Ibidem, pp. 14-15.

¹⁹⁸ Ibidem, pp. 16-17.

A existência da rede mundial em escala gigantesca e da falta de controles internacionais, além de a falta de cooperação entre as soberanias gera simultaneamente dois problemas: por um lado, se o local em que os efeitos do crime foram sentidos for diverso do local da prática delinquente, é de se verificar se há algum modo de fazer com que o delinquente seja investigado, coibido e punido, pois muitos países ainda não possuem legislação própria no sentido penal para o tema. Um outro problema é o fato de que com a demora no encontro do delinquente ou da máquina utilizada, diversas pistas já foram destruídas ou não foram adequadamente preservadas.

As prevenções primária e terciária também se mostram deveras ineficientes na temática. Isso porque se acredita que o cidadão delinquente virtual compreende o caráter ilegal de suas ações, tem boa educação e até boas condições sociais. Do mesmo modo, não se pode dizer em necessidade de ressocialização para o criminoso voluntário que pratica o fato imiscuído de motivos que não raro não se encaixam em qualquer das teorias criminológicas, mas sim em teorias de anulação de responsabilidade ou de técnicas de neutralização, utilizadas pelos desviantes.

De acordo com o estudo desenvolvido por Sykes e publicado na *American Sociological Review* 22 em 1957, certas ações criminosas (informáticas inclusive) carecem de explicação criminológica para seus acontecimentos. Isso porque a violação de um valor social, de uma norma de bom convívio é latente, o delinquente tem consciência disso, mas ainda assim comete o ato, deixando as teorias criminológicas puras tenhas dificuldades em explanar tais ações. Por isso, desenvolveu o raciocínio de que alguns comportamentos são justificados por chamadas técnicas de neutralização que permitem que o agente temporariamente neutralize valores, crenças e atitudes de aceitação comum para legitimar um comportamento.

Orly Turgeman-Goldschmidt focou-se nas ações *hackers*¹⁹⁹ e, utilizando-se da construção de Sykes concluiu que as justificativas apresentadas pelos delinquentes informáticos com frequência altíssima utilizam-se de tais técnicas.

Cinco são as técnicas de neutralização: (a) negação de responsabilidade; (b) negação de

¹⁹⁹ TURGEMAN-GOLDSCHMIDT, Orly. The Rhetoric of *Hackers' Neutralizations in Crimes of the Internet* (Org. SCHMALLEGER, Frank e PITTARO, Michael). Pearson Prentice Hall, New Jersey, EUA, 2008, pp. 317-

prejuízo; (c) negação de vítima; (d) condenação dos condenador; e (e) apelo a valores superiores. No primeiro caso, culpam-se forças além do controle do vitimário para justificar a ação. No segundo caso, a justificativa está no fato de que a ação não gerou prejuízo considerável à vítima. O terceiro caso trata da ideia de retaliação ou devolução de um sofrimento merecido à vítima. A condenação do condenador é a tentativa de reversão da culpa da atitude, atribuindo-se o legislador e a lei penal como duvidosos em sua ação ou legitimidade. Finalmente, o apelo a valores superiores aponta a atitude como sacrifício para priorizar valores mais importantes ao agente²⁰⁰ como uma crença ou um ideal político.

As atitudes ciberdelinquentes admitem a aplicação de tais técnicas de neutralização. Vejamos: os ciberdelituosos não raro informam que suas ações não geram e sequer gerariam qualquer prejuízo às vítimas, porque num ambiente virtual, as ações também seriam imateriais e eventuais prejuízos, inquantificáveis. Certas atitudes seriam tomadas contra usuarios sob pretexto de que houve merecimento, isso porque os expertos atribuem-se o apelido de justiceiros ou participantes de uma cruzada pela justiça, punindo ações irresponsáveis, partidos de oposição ou religiões diversas. Quando se fala de condenação a condenadores, o que se diz é que algumas atitudes visam demonstrar aos principais poderes da federação a discordância quanto a atitudes e quanto às criações legislativas *a contrario sensu* da opinião da maioria dos usuarios, numa exposição do fracasso prático da democracia indireta, recusando obediência a leis de aceitabilidade duvidosa. Finalmente, há quem diga que certos valores e lealdades chegam a estar até acima de leis e normativos, sendo obrigação dos indivíduos, ao deparar-se com a alternativa de descumprir a lei e desrespeitar seus valores, sempre deve escolher a primeira opção.

318.

²⁰⁰ Ibidem, p. 318

O AUTOR DO DELITO INFORMÁTICO

Em primeira impressão, a análise do autor do delito informático pode parecer fugir da temática proposta no trabalho. Poder-se-ia argumentar que um trabalho sobre vítimas não deve ater-se a raciocínios comportamentais da psiquiatria ou psicologia do criminoso. Porém, o foco da tese esposada não se atém ao Direito Penal mas sim ao estudo criminológico da vítima e de todo o universo nela envolvido.

A criminologia, como ciência que exige um raciocínio completo da situação-delito, demanda ser compreendida em todos os seus aspectos e analisada como um fenômeno normal para que seja possível buscar modos de diminuir sua incidência e prevenir parte dos acontecimentos, entendendo a fundo a realidade. Foi a ciência responsável pela criação de teorias do autor e que serve de porta de entrada para o raciocínio vitimal. É, aliás, expressão de Hassemer, a de que *“quem não encontra uma vítima apropriada, não pode ser autor”*²⁰¹.

Ainda que superados e contraditos os critérios do positivismo jurídico inaugurado por Lombroso e que davam à ciência biológica força para submeter as regras de imputabilidade do Direito Penal à uma lógica atávica, é natural que ao se tratar de delitos informáticos (próprios e mormente impróprios) considere-se que existe um perfil médio para tal delinquente.

A partir do momento em que se parte do pressuposto de que há a necessidade de instrumentos informáticos para o cometimento do delito, é natural que se leve em conta as particularidades deste bem jurídico e desta ferramenta.

De acordo com o Dicionário Virtual Michaelis, a informática é *“o ramo através da qual ocorre o tratamento da informação, ou seja, o emprego da ciência da informação”*²⁰² com o computador eletrônico”.

²⁰¹ HASSEMER, Winfried. Introdução aos Fundamentos do Direito Penal. Sergio Antonio Fabris Editor, Porto Alegre, 2005, p. 110.

²⁰² Definição surgida nas conferências do *Georgia Institute of Technology*, EUA, realizadas em Outubro de 1961 e Abril de 1962, retomada e republicada por Harold Borko em 1968: *É a disciplina que investiga as propriedades e o comportamento da informação, as forças que regem o fluxo informacional e os meios de processamento da informação para a otimização do acesso e uso. Está relacionada com um corpo de conhecimento que abrange a origem, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação. Isto inclui a investigação, as representações da informação tanto no sistema natural, como no artificial, o uso de códigos para uma eficiente transmissão de mensagens e o estudo dos serviços e técnicas de processamento da informação e seus sistemas de programação.* Acesso em

Os equipamentos eletrônicos hoje existentes com os quais mais se praticam condutas reprováveis são os computadores de mesa, os aparelhos celulares e os *notebooks*. Sem prejuízo à campanha de redução de preços e impostos dos insumos informáticos existente sazonalmente no país, ainda hoje a aquisição de uma máquina exige algum poder aquisitivo. Também, para o manuseio de tais ferramentas há que se desenvolver capacidade de digitação, além de ser requisito importante a compreensão da língua inglesa para o uso amplo dos sistemas, sem contar, certamente, o conhecimento da linguagem especial para manuseio dos programas²⁰³.

Diante de tais afirmações, é de se concluir que ainda que não se possa dizer haver um perfil biológico para um delinquente informático, é certo que somente pessoas com certo poder aquisitivo, certa educação para língua estrangeira e considerável capacidade de digitação são capazes de se mostrarem proficientes para a prática de boa parte dos delitos que exigem capacidade técnica.

Para Roberto Chacon de Albuquerque, delitos informáticos são condutas da modalidade colarinho branco porque só um determinado número de pessoas, com certos conhecimentos técnicos podem chegar a cometê-los²⁰⁴.

É fatídico que a disseminação informática não tem regresso. Resta-nos compreender quem dentro deste universo cada vez mais popular propõe-se a agir de modo delinquente e quem estará mais propenso a ser violado. Acerca da situação do usuário de informática, analogamente, Sérgio Salomão Shecaira aponta que

“Assim, o habitante da cidade (aqui entendido como os usuários do ciberespaço) se adapta mediante uma conduta que implica uma tendência a agir de maneira segmentada e funcional, isto é, com predomínio de relações secundárias; esse morador tem o desenvolvimento de uma postura de impessoalidade, distanciamento e não envolvimento com as pessoas; (...). Vale

<http://www.ccje.ufes.br/dci/deltci/def.asp?cod=15> em 09.04.08, às 00:01hs.

²⁰³ O CERT.BR – Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil – desenvolveu uma cartilha denominada “cartilha de segurança para a Internet” que, em seu capítulo final apresenta um glossário de termos mínimos da linguagem informática para a compreensão dos incidentes de segurança referidos. Esta cartilha está disponível em <http://cartilha.cert.br/glossario/>. Acesso em 09.04.08, às 10:46hs.

²⁰⁴ ALBUQUERQUE, Roberto Chacon de. Op. cit. p. 11.

dizer, adota uma postura basicamente individualista (...)²⁰⁵”

Conforme já apresentado acerca de a rede ser composta de uma infinidade de usuarios potencialmente conectados, soma-se a ideia de anonimato com o sentimento de intangibilidade e é correto assumir o posicionamento de Sándor Ferenczi de que

“Na multidão, o homem converte-se em criança, sente-se irresponsável pelas ações, em relação às quais somente o líder, investido de um poder quase paternal, assume a responsabilidade”²⁰⁶

Certo é que apesar de a cada dia mais perceber-se que a criminalidade informática não exige indivíduos com características particulares – muito especialmente pelo fato de que diversos dos delitos informáticos poderem ser perpetrados sem qualquer habilidade – ainda assim prevalece na figura do delinquente de alto gabarito, boa quantidade de conhecimento de informática, mais especialmente naqueles delitos que envolvem programação e intrusão.

Boa parte dos delitos perpetrados têm como responsáveis usuarios com alguma relação empregatícia com os alvos de ataque, inclusive permitindo a incidência em tese da agravante do artigo 61, II, “g” (violação de dever inerente a cargo, ofício, ministério ou profissão) nas figuras dos *insiders*²⁰⁷ que por vezes buscam vingança de seus empregadores, meros prejuízos ou até mesmo lucros e vantagens por conhecer as fragilidades da empresa.

Certo é que a grande distância que a informática gera e mantém entre as pessoas encoraja ações mais agressivas e menos comportadas tanto por parte do vitimário quanto por parte da vítima. A aqueles pela ousadia e pressuposição de impunidade e a estes por conta de

²⁰⁵ SHECAIRA, Sergio Salmomão, *Criminologia*, 2ª Edição. Editora RT, São Paulo, p. 157.

²⁰⁶ Sándor Ferenczi *apud* SHECAIRA, Sergio Salmomão, Op. cit., p. 162.

²⁰⁷ “(...) veremos que a figura do delinquente não apresenta características específicas. Muitos crimes podem ser praticados através dos meios informáticos, de forma que, em muitos casos, tais sujeitos realmente não necessitam ter conhecimentos especiais para consumá-los. São indivíduos de diversos níveis culturais e intelectuais. Na realidade, trata-se de pessoas com razoáveis conhecimentos de informática, pois a maioria das fraudes informáticas são realizadas mediante complexas manipulações. Com isso, alguns requisitos são exigíveis com respeito à pessoa do agente. Tampouco isso quer dizer que sejam superdotados ou algo parecido. A esse respeito a própria doutrina admite que os autores de crimes informáticos são, geralmente, funcionários de empresas ou técnicos informáticos, pois têm acesso aos sistemas informatizados das empresas para as quais trabalham” Deduz-se, portanto, que são pessoas qualificadas, fato que incrementa ainda mais a vulnerabilidade do sistema” CRUZ, Daniele Rocha, p. 17

segurança e porque maiores ousadias na navegação virtual geram maior vulnerabilidade, mais alta exposição ao risco sob a sensação de tranquilidade e frieza.

Foi o surgimento gradual da criminologia que promoveu verdadeiro chamar de atenção para a imprescindibilidade da interpretação fática por um viés da figura do criminoso. Acresceu-se à conduta delitiva, com o desenvolver de uma criminologia clássica, o estudo do próprio delinquente, chamando-se a atenção para raciocínios como o do motivo pelo qual uma pessoa se torna criminosa, mormente denominado elemento subjetivo do tipo. Não é errado dizer que o positivismo jurídico deu um colorido concreto no pensamento criminal, aproximando-o a ideais empíricos, reais e dinâmicos.

Quando o assunto é criminalidade informática, diversos pensamentos justificantes tentam apontar para uma lógica delinquente. Pacífico é o fato de que há uma volumosa preponderância de delinquentes virtuais do sexo masculino, ideia essa que é reforçada por uma questão lógica: há muito mais usuarios homens do que mulheres e a maioria dos usuarios têm verdadeiro gosto por tecnologia.

Diz-se em análise psicológica do tema, que o submundo informático é povoado por homens jovens e solteiros que vivem fantasias de glória e poder através do uso de um teclado e que estão dispostos a substituir a atividade sexual saudável, tendo-se em vista que sua principal companhia é sua máquina²⁰⁸. A este perfil de delinquente, é atribuído a criação de códigos maliciosos os quais são criados (*rectius*: escritos) pelo usuario que os trata como filhos da união deste indivíduo o seu dispositivo – como na mitologia em que Pigmaleão

²⁰⁸ Não é de tudo errado, em nossa opinião, acreditarmos que a informática e o conseqüente isolamento dos indivíduos atrás das máquinas é resultado ao menos indireto da criação de uma sociedade do medo, em que os meios de comunicação propugnam e disseminam notícias de violência – urbana, de trânsito, doméstica, internacional, etc –, de caos e de histeria, levando o ser humano a consumir artigos da indústria da segurança privada em detrimento à confiança na segurança pública, que cai naturalmente. Também, o usuario passa a optar pelo evitamento de riscos crescentes e constantes nas ruas, migrando as atividades para o uso da informática, que provém um meio preservativo quanto a alguns dos temores. Neste sentido, acreditamos que a violência não raro é interpretada como meio de marketing e venda de produtos midiáticos, pois a sociedade, no intuito de se preservar e se educar quanto aos problemas e dificuldades de vivência termina por consumir tais produtos sensacionalistas. Neste sentido, <http://noticias.uol.com.br/ultnot/efe/2005/08/08/ult1766u11336.jhtm>. Acesso em 26.09.08, às 14:37hs. No mesmo sentido, mas com abordagem quando ao temor pela situação econômica no mundo a partir da crise dos créditos podres dos Estados Unidos da América do Norte, *podcast* e arquivo de áudio sobre a crise financeira pode ser encontrado no site: http://cbn.globoradio.globo.com/cbn/wma/player_gradio.asp?audio=2008/colunas/fatofoco1_080920.wma&OAS_sitepage=sgf/sgf/radioclick/radiosam/cbn/fato1. Acesso em 26.09.08 às 14:39hs referente ao programa “Fato em Foco” que se propõe a discutir o papel e a responsabilidade da mídia na sociedade.

apaixona-se por sua escultura Galatéia, o *geek* se apaixona por seu vírus.

A frequência a grupos de discussão de *hackers*, por exemplo, em pesquisa empírica, revela que há uma relação entre a sexualidade e as práticas informáticas invasivas pressupondo-se que há um sentimento generalizado de feminização da virtualidade.

Os sistemas informáticos seriam interpretados como uma figura feminina desconhecida e que desperta desejos de invasão e penetração forçada por parte de alguns usuarios que nela navegam; por isso, o numeral de homens cometedores de delitos relacionados a invasão, controle e domínio seria justificável a partir de tal conceituação instintiva. Nas citações de Paul A. Taylor ao analisar depoimento de membro do *Toxic Shock Group*:

*“(...) nós hackeamos e hackeamos um sistema como um homem em um safari, limpando a mata da floresta com seu machete, tentando atingir um destino que ainda não conseguimos visualizar. Nós desejamos ardentemente, torturando nossos cérebros e batendo os dedos no teclado, até que finalmente, oh num doce finalmente, conseguimos ingressar”*²⁰⁹

Não se pode esquecer neste ponto que o ciberespaço é representado pelo codinome “MATRIX”, palavra de origem latina e que significa “matriz”, “mãe” ou “útero” e que, pois, em uma perspectiva freudiana, poderia ser um ambiente em que o usuario se sente seguro, protegido e que pode chegar até mesmo a ser objeto de obsessão e violência²¹⁰.

Some-se a isso a ideia machista de que o ciberespaço poderia ser comparado a uma terra sem lei, auto-regulamentar como o velho oeste em que os mais fortes prevalecem e determinados estereótipos masculinos afloram-se²¹¹.

Outro ponto curioso acerca da personalidade do ciberdelinquente é a ideia de que o

²⁰⁹ TAYLOR, Paul A. Maestros or Misogynics? Gender and the social construction of hacking. In Dot.cons.. Willan Publishing. Londres. 2002. p.133 “we hack and hack at a system like a man on a safari, clearing away the vines of the jungle with his machete, trying to forge ahead a destination he cannot yet see. We keen on, torturing our brains and pounding our fingers on the keyboard until at last... oh at long, sweet last... we are in.”

²¹⁰ Falando sobre teorias psico-sociais dos hackers, TAYLOR, Paul A. Maestros or misogynists? Gender and the social construction of hacking. In Dot.Cons (editado por Yvonne Jewkes). Willan Publishing, Devon, 2002, pp. 133-134.

²¹¹ *Ibidem*, p. 128.

ciberespaço pertence aos verdadeiros “*netizens*” (neologismo para cidadão da Internet pela fusão das palavras *net* e *citizens*), cidadãos da era informacional preparados para enfrentar a nova realidade e que desprezam os usuarios amadores, eventuais e meramente utilizadores da rede como ferramental. A partir de seus conceitos, a rede (quicá autopoietica) é capaz de destruir e expulsar aqueles que não forem capazes de se adaptarem a ela. Por isso, existiria na rede, afora a auto-regulamentação, uma espécie de darwinismo digital em que somente os mais fortes sobreviveriam, somente os mais capazes de sobreviver às intempéries virtuais seriam dignos de manter-se no meio. Tais posturas são permeadas por ataques constantes com intuits destrutivos como finalidade seletiva²¹². A esse perfil de usuarios deu-se o nome de *ciberpunks* ou tecnolibertarianos²¹³.

Não há dúvida que se estereotipou o criminoso informático, chegando-se até mesmo a um perfil considerado comum. Seria *hacker* um indivíduo do sexo masculino, brancos, não violento, de família de classe média alta, sem antecedência criminal, e com idade média de 24 anos²¹⁴.

Diante disso, é de se crer que não se pode generalizar a figura do delinquente quanto a sexo, idade e classe social, exceto pelo fato de que todos acabam por ter conhecimentos de língua estrangeira, gosto por tecnologia, capacidade de digitação e algum potencial aquisitivo para a obtenção de maquinário ou acesso a dispositivos direta ou indiretamente²¹⁵.

²¹² Comparativamente a tais ideias está o pensamento social de Herbert Spencer (1820-1903) que, de acordo com Sergio Salomão Shecaira “*fez uma analogia entre o funcionamento de um fígado e o da cidade de Manchester. Em seu ultraliberalismo, Spencer chega a afirmar que os pobres, imprudentes, incapazes, débeis, enfiam fracos, em geral, seriam superados pelos mais aptos*” (Criminologia. Editora RT. 2008. São Paulo, p. 91).

²¹³ TAYLOR, Paul A. Op. cit. pp. 138-139.

²¹⁴ Porém, não há de se deixar de levar em conta o fato de que tal padronagem não encontra guarida científica, especialmente se levar em conta o fato de que há duas naturezas distintas de delinquência na área: a própria e a imprópria, sendo a segunda aquela que representa a criminalidade comum, somente praticada pela ferramenta eletrônica.

²¹⁵ Deve-se levar em conta, também, que a personalidade e os objetivos do delinquente fizeram com que diversas nomenclaturas os classificassem. Assim, “*hacker*” seria o conhecedor de informática e tecnologias, capaz de utilizá-las além dos limites básicos, não necessariamente com intuits prejudiciais; “*cracker*”, por sua vez, seria uma modalidade de “*hacker*”, mas com objetivos criminosos de violação de bens jurídicos informáticos para obter vantagens; “*sniffer*” seriam usuarios familiarizados com o uso de programas de interceptação de dados como *emails* e outras informações sensíveis (até por meio de *malwares* armadilha). A figura do “*spammer*”, por sua vez, trata do usuario que envia indiscriminadamente e em grande quantidade, mensagens não solicitadas, comerciais ou não, com intuito de divulgar produto, propagar imagem, etc. Restam ainda as figuras do “*stalker*” – que é alguém que persegue outrem através dos meios informáticos e o vigia, perturbando e ameaçando indiretamente –, do “*bullier*” – indivíduo que amedronta outros mais fracos com ameaças e ofensas –, e até o

O estudo da vitimologia detém-se na figura da relação intrínseca entre o criminoso e sua vítima que vai desde o entrosamento, complexidade e cooperação entre ambas figuras até a propensão da vítima a cumprir com esse papel. Por isso, o único modo de se compreender perfeitamente o delinquente, está no estudo paralelo daquele que com ele reage pois que da mesma forma que há um *iter criminis* em que se analisa as etapas do comportamento externo e interno do delinquente, também há um *iter victimae* e a relação entre ambos é muito próxima.

A psicologia forense, especialmente aquela ligada à investigação psicológica da personalidade da conduta criminosa, em detido estudo feito pela cátedra do Dr. Antonio de Pádua Serafim, professor doutor da Faculdade de Medicina da Universidade de São Paulo, concluiu que há um processo de identificação do comportamento anti-social além do *iter criminis* para a execução de um fato típico.

Tal processo consistiria em três etapas a serem descobertas pelo profissional da psicologia quanto a um crime, sendo tais (i) a capacidade de compreensão da ação anti-social por parte do delinquente e a identificação dos motivos da prática – denominada MOTIVAÇÃO; (ii) a oportunidade fática em que estava inserido o delinquente – CIRCUNSTÂNCIAS; e o panorama dos comportamentos anteriores do indivíduo – HISTÓRICO DELINQUENCIAL²¹⁶.

Para nós, são as circunstâncias no que se refere à oportunidade de um indivíduo delinquir que nos importam, visto que para nós, há que se completar tal tarefa a partir do estudo das ações anteriores ao fato, as ações no momento do fato, e as reações ao fato, todas conjugadas com a ideia de que há um papel da vítima na construção do delito, há responsabilidades dela frente à vida que leva e os riscos que corre e há deveres de cuidado presumidos.

“ciberterrorista” – que é o usuário que, guiado por crenças, fundamentalismos, religião ou até mesmo política, promove ataques contra *sites* e sistemas que colidem com suas ideias.

²¹⁶ SERAFIM, Antonio de Pádua. Aspectos Etiológicos do Comportamento Criminoso: parâmetros biológicos, psicológicos e sociais. In: Sergio Paulo Rigonatti; Antonio de Pádua Serafim; Edgar Luiz de Barros. (Org.).

VITIMOLOGIA E VITIMODOGMÁTICA

O mote deste trabalho não se resume na abordagem acerca da nova criminalidade e nem busca propriamente o criminoso; quer-se demonstrar a importância da compreensão da vítima informática e sua relevância na construção do delito informático.

Para tanto, mesmo que sendo lugar comum na maioria dos doutrinadores da área, mister que se compreenda a vitimologia percorrendo seu desenvolver ao curso da história e suas nuances, especialmente quanto às ideias de tendência dos usuarios de dispositivos tecnológicos em se tornarem vítimas bem como sua contribuição no delito.

A maior parte da doutrina acredita que a vitimologia é um braço da criminologia, apesar de alguns defenderem que deveria ter autonomia principiológica e em seus estudos²¹⁷. Contudo, por conta de sequer a criminologia contar, na doutrina nacional, com a condição de ser considerada ciência autônoma mas apenas ramo auxiliar do Direito Penal, os principais ícones pensadores acabaram por aceitar o estudo da vítima como parte da forma de correta compreensão da ecologia criminal²¹⁸. Assim, estudar a vítima e seus aspectos é dedicar-se a um ramo da criminologia crítica que, nos dizeres de Antônio Garcia Pablos de Molina é

“Ciência empírica e interdisciplinar que se ocupa do estudo do crime, da pessoa do infrator, da vítima e do controle social do comportamento delitivo, e que trata de subministrar uma informação válida, contrastada, sobre a gênese, dinâmica e variáveis principais do crime, assim como sobre os programas de prevenção eficaz e técnicas de intervenção positiva no homem delinquente e nos diversos modelos ou sistemas de resposta ao delito.”

Temas em Psiquiatria Forense e Psicológica Jurídica. 1ª. edição. Vetor Editora, São Paulo, 2003, p. 49-64.

²¹⁷ MENDELSON foi o principal defensor de tal ideia, segundo NEUMAN e OLIVEIRA. Também tendente à autonomia, Edgard de Moura Bittencourt. Houve, inclusive, especial atenção a tal proposta, que foi objeto do Relatório Geral do 7º. Simpósio Internacional de Vitimologia, realizado no Rio de Janeiro em agosto de 1991. OLIVEIRA, Ana Sofia Schmidt. Op. cit. pp. 88-89 e p.92; NEUMAN, Elias. Op. cit. pp. 36-37.

²¹⁸ Expressão utilizada por Robert F. Meier, Terance D. Miethe. MEIER, Robert F. e MIETHE, Terance D. Understanding Theories of Criminal Victimization. In Crime and Justice, v. 17. The University of Chicago Press, Chicago, 1993, pp. 459-499.

Diz-se que a criminologia teve seu início com Cesare Lombroso²¹⁹, por volta do século XIX, e sua iniciativa de, através da caracteriologia – mais especialmente a cranioscopia e a frenologia²²⁰ – estudar a relação entre as diferentes características dos indivíduos e sua propensão em tese genética para o cometimento de delitos²²¹.

Tais estudos aumentaram o espectro de raciocínio existente nas academias, antes restritas e centradas no estudo causal do fenômeno delituoso e seu resultado como fato jurídico modificador da realidade.

A partir da nova proposta, direcionou-se o olhar também para a figura do criminoso, que pressupostamente era irresponsável por sua conduta, por ser uma espécie de ser humano fruto da evolução genética, numa repetição de características e más-formações de seus antepassados, e que resultariam no cometimento irracional de crimes²²².

Na mesma época, Enrico Ferri e Raffaele Garófalo contribuíram para o estudo do delinquente, pela escola positivista italiana, estudando as causas do delito e os tratamentos mais adequados. A partir deles, o estudo penal passou por uma grande mudança.

Em curtas linhas, Enrico Ferri defendeu que as ciências sociais eram responsáveis pela compreensão da criminalidade, reforçando a tese de que o delinquente não possui livre arbítrio pois é fruto da sociedade em que vive; Raffaele Garófalo, por sua vez cria na antropologia do crime, que partia sempre dos indivíduos, aquilo que denominou *temibilidade*, inerente a cada um pela violação de sentidos morais²²³.

A vitimologia de hoje se desenvolveu a partir das conflagrações mundiais, com a precariedade econômica pós-guerra, com a “guerra fria” e especialmente os estudos pós-

²¹⁹ Sérgio Salomão Shecaira apresenta que, em verdade, Lombroso foi capaz de tornar científica e popular a publicação de seus estudos, mas que, contudo, diversos outros estudiosos precederam o médico nos estudos caracteriológicos como, p. ex., Giovanni Battista Della Porta Vico Equense, Johan Caspar Lavater, Petrus Camper, Franz Joseph Gall, dentre tantos outros. In SHECAIRA, Sergio Salomão. Criminologia. 2ª Edição. Editora Revista dos Tribunais. São Paulo. 2008. pp. 81-108

²²⁰ Caracterologia é o estudo do caráter e da personalidade, e o seu desenvolvimento diferenciado nos diferentes indivíduos; a frenologia, por sua vez, é a teoria segundo a qual as faculdades intelectivas, afetivas e instintivas do indivíduo têm relação com as fossas ou depressões cranianas.

²²¹ SABBATINI, Renato M. E.. “Cesare Lombroso – Uma breve biografia”. Revista Cérebro e Mente in <http://www.cerebromente.org.br/n01/frenolog/lombroso.htm> Acesso em 08.08.08 às 21:46hs.

²²² Denominou-se tal fato de atavismo, numa espécie de predestinação criminal pela repetição de características ao longo de gerações.

segunda guerra mundial – período de macrovitimizações causadas pelo genocídio judeu e pela bomba atômica no Japão –, em especial feitos por Hans von Hentig e pelo médico judeu Benjamin Mendelsohn, este que em 1947 profere uma conferência intitulada “*Um horizonte novo na ciência biopsicossocial*”. Quiçá impulsionado e percebido por conta de um possível e notório ciclo histórico de perseguição ao povo hebreu²²⁴, Benjamin Mendelsohn inicia questionamento acerca da ausência da vítima no estudo do delito, responsabilizando a falta de tal raciocínio a uma compreensão incompleta do fenômeno delitual.

Propõe que se inicie a focar o fato crime interpretando-o também a partir da vítima, tanto em momento anterior ao cometimento como em momento posterior, na fase de comunicação do fato à autoridade pública e até mesmo após a apuração e punição, numa ação compensatória e reparadora.

Tal enfoque leva a criminologia a aumentar sua complexidade, posto que mais do que estudar o crime e seu agente causador, mostra-se perspicaz a ideia de que a conduta da vítima no cotidiano, bem como sua educação, são propensões que contribuem para o acontecimento dos crimes.

Da mesma maneira, o estudo focado da vítima mostra que a simples prevenção – seja geral ou específica – destinada a impedir que o delinquente incida em tipos penais, é insuficiente, posto que muitas vítimas não compreendem que em muitos casos são verdadeiros agentes provocadores.

A presença da vítima, nos mais diversos delitos, chega a ser fundamental para o acontecimento do fato, porquanto diversos tipos exigem interação entre vítima e vitimário, como o estelionato, por exemplo.

O estudo detido da vítima dos crimes mostra-se simultaneamente importantíssimo e muito árduo. Importantíssimo porque novos aspectos passam a ser observados como a relação de contribuição da vítima para o cometimento do delito, a forma de sua escolha por parte do

²²³ SHECAIRA, Sergio Salomão. Criminologia. 2ª Edição. Editora RT, São Paulo, 2008, pp. 104-106.

²²⁴ Apenas a título de exemplo, no ano 66, em Alexandria (Egito), houve o primeiro massacre registrado dos judeus. A partir daí, outras perseguições e matanças ocorreram: Constantino, por razões políticas, se converteu ao equivalente ao cristianismo em Roma em 324 d.C., e declarou guerra contra o povo judeu; no século XI, a primeira cruzada promove um massacre aos judeus; no final do século XIII, os ingleses expulsam os judeus do

criminoso, os locais mais propensos para a vitimização, as relações da vítima com o ofensor, sua necessidade de sua prevenção e educação, etc. A teoria da imputação objetiva permite que diversos resultados tenham sua imputação atenuada frente ao autor ou mesmo negada por conta de ter havido contribuição causal da vítima para o acontecimento²²⁵.

A dificuldade do estudo, por sua vez, se dá principalmente pelo problema da evolução do conceito de vítima que passa a ser abordado, em breves linhas.

É repetido pelos mais diversos doutrinadores-vitimólogos, e com especial atenção, por Ana Sofia Schmidt de Oliveira, Guilherme Costa Câmara e por Tony Kearon e Barry S. Godfrey, que a vítima teve seus tempos áureos na história da humanidade²²⁶.

O estudo do evoluir das formas de resolução de conflitos passa por três momentos de prevalência, quais sejam a fase da autotutela, a fase da autocomposição e, por fim, a presente fase da jurisdição.

Certamente que não de forma estanque, o evoluir das formas de resolução não implicou, em verdade, a abolição do modo anterior. Assim, a existência da jurisdição hodierna não restringiu totalmente as possibilidades de os cidadãos autotutelarem-se em alguns casos, bem como autocomporem-se²²⁷.

A autotutela, método originário de resolução de conflitos, revelou-se o modo que maior força deu à vítima: permitia que o lesionado reagisse, fosse no momento imediatamente posterior à agressão, fosse em qualquer outro momento, da forma como bem entendesse, para

país, que seguem sendo expulsos dos países europeus; entre muitos outros exemplos.

²²⁵ SILVA SANCHEZ, Jesús Maria. “La consideracion del comportamiento de La victima em La teoria juridica Del delito”. *Revista Brasileira de Ciências Criminais*, Nº 34, Ano 9, Abril-junho de 2001, Editora Revista dos Tribunais, São Paulo, 2001, p. 169.

²²⁶ OLIVEIRA, Ana Sofia Schmidt de. Op. cit. pp. 17-32; KEARON, Tony e GODFREY, Barry S. Setting the scene: a question of history. In *Handbook of Victims and Victimology* (Ed. Sandra Walklate). Willan Publishing, Devon, 2007, pp. 18-22. Também neste sentido, Jesús-María Silva Sánchez in “La consideracion del comportamiento de La victima em La teoria juridica Del delito”. *Revista Brasileira de Ciências Criminais*, Nº 34, Ano 9, Abril-junho de 2001, Editora Revista dos Tribunais, São Paulo, 2001, pp. 163-165; CÂMARA, Guilherme Costa. Op. cit., pp. 21-61.

²²⁷ Remanesce o direito de autotutela no Direito Penal, em institutos como o da retorsão imediata nos casos de injúria verbal e na legítima defesa, por exemplo. No caso de autocomposição, é exemplo a possibilidade de transação penal e até de composição de danos no rito sumário inaugurado pela Lei 9.099/95.

reparar seu prejuízo – moral, jurídico ou até patrimonial – de acordo com sua própria força ou com a força que pudesse obter para auxiliá-lo²²⁸. A sociedade estimulava a reação da vítima²²⁹.

A vítima do delito, portanto, era livre para reagir como entendesse, tendo, pois, papel fulcral na resolução do conflito, que somente cessaria após a realização da vontade vitimal, que poderia também ser a de não retribuir o mal causado.

Era a fase do predomínio da importância da vítima na relação violadora, pois a consequência de o cometimento de um delito era a geração automática de um direito ao lesado. Período histórico de ausência de centralização de Estado, a sociedade importava-se mais com a figura daquele que foi violado em seus direitos do que com o fato em si, além de pugnar pela defesa da coletividade ameaçada e tornada inquieta. A reação do vitimado era o objeto central da sociedade que podia, inclusive, fazer prevalecer a vítima frente ao delinquente na sociedade, fosse expulsando-o da célula social, fosse capturando o agente para impor-lhe a reação que cabia a vítima.

A sociedade antepassada parcialmente organizada, inclusive, chegou a positivar tábuas de direitos em que há nítida prevalência da vítima na relação delinquente. É o caso do Código de Hamurabi, considerado o principal ícone da justiça privada autotutelar com a filosofia da compensação de culpas: qualquer que fosse o ato praticado, se lesivo, geraria imediata permissão para que a vítima da primeira ação prejudicial devolvesse “na mesma moeda” o prejuízo sofrido.

Havia forte diferenciação de classes de cidadãos, que tinham pesos diferentes na ponderação da justiça²³⁰. Homens livres eram considerados detentores de mais direitos que escravos; mulheres eram juridicamente inferiores a homens e assim sucessivamente. Por isso,

²²⁸ Um filme interessante acerca da autotutela é “Abril Despedaçado”, de Walter Salles (distribuição Miramax Films) em que um pai manda seu filho vingar a morte de seu irmão, matando o assassino da família rival, que há gerações vive na disputa pela terra no nordeste. O filho sabe que ao matar, passará a ser perseguido, numa repetição de vinganças das famílias, em autotutela. No mesmo sentido, CÂMARA, Guilherme Costa. Op. cit., p. 25-27 e p. 33-35.

²²⁹ OLIVEIRA, Ana Sofia Schmidt de. Op. cit. pp. 21 e ss.

²³⁰ Aqui cabe citar a figura jurídica do “*wergeld*”, que poderia ser explicado como o montante de pecúnia que deveria pagar o injuriador para a família da vítima do crime de homicídio como quantidade financeira representativa do valor do morto.

apesar de se considerar aquela doutrina a do “olho por olho, dente por dente”, ainda assim o Princípio da proporcionalidade era relativizado.

Violações a vítimas de mesma classe social geravam vingança idêntica ou de maior intensidade – num embrião de retribuição e prevenção como fins da pena – e violação de vítima de classe social diferente geraria reação nada isonômica em nossos moldes atuais, como nos exemplos abaixo:

“196º - Se alguém arranca o olho a um outro, se lhe deverá arrancar o olho.

197º - Se ele quebra o osso a um outro, se lhe deverá quebrar o osso.

198º - Se ele arranca o olho de um liberto, deverá pagar uma mina.

199º - Se ele arranca um olho de um escravo alheio, ou quebra um osso ao escravo alheio, deverá pagar a metade de seu preço.

200º - Se alguém parte os dentes de um outro, de igual condição, deverá ter partidos os seus dentes.

203º - Se um nascido livre espanca um nascido livre de igual condição, deverá pagar uma mina.

205º - Se o escravo de um homem livre espanca um homem livre, se lhe deverá cortar a orelha.²³¹”

Enfim, a sistemática do Código de Hamurabi e de outras positavações, faz com que a vítima tenha seu direito reconhecido imediatamente, e, portanto, figure como protagonista no momento da punição de um cidadão por um ato ilegal. Diz-se que o principal objetivo do Direito Penal da época é a garantia à vítima de retribuição e recomposição²³².

²³¹ Código de Hamurabi: Código de Manu, excertos (livros oitavo e nono): Lei das XII Tábuas (supervisão editorial Jair Lot Vieira). 2ª Edição. EDIPRO, Bauru, 2002, pp.30-31.

²³² Ainda hoje, sociedades silvícolas permanecem com ideais autotutelares, dando ao lesado o direito de revanche e, em certos casos, até mesmo expulsando o delinquente da aldeia.

Seguinte à autotutela, com o evoluir da sociedade quanto a tecnologias e ferramentas e com a maior capacidade de cultivo, criação e estabilização sedentária, surgem sensações mais sólidas de bens jurídicos e de interesses em maior segurança e pacificação social. Ofensores e ofendidos desenvolvem em sua intelectualidade a ideia de transacionar o direito lesado, evitando-se castigos corporais, mortes e diminuindo instabilidades. A partir da oitiva dos interesses da vítima ou a partir de patamares de composição pré-determinados, compensava-se o ofendido para reduzir-lhe as perdas advindas da violação.

Com o fortalecimento e focalização de um poder central, reforçado por ideias lucrativas como a de centralizar-se a figura da pacificação social através de autoridades saneadoras de conflito que, assim, gerariam capital para o Estado, surgiram figuras de julgadores, como os pretores, que tinham função de avaliar o conflito das partes e determinar a forma de resolução do conflito.

Como apresentado por Tony Kearon e Barry S. Godfrey, na sociedade anglo saxônica, nos tempos do rei Alfred (871-99), o Estado emergente iniciou movimentos mais explícitos para tornar-se o determinador da aplicação da lei e das punições e, em alguns casos, poderia obrigar o delinquente a pagar não só um valor compensatório para a vítima mas também para o mesmo valor para o rei (denominado “*wite*”- vergonha, vexame)²³³. Em dado momento, todo o *jus puniendi* estava concentrado na mão do poder central²³⁴. Todavia, as acusações e os julgamentos não possuíam proporcionalidade ou igualdade e variavam com frequência, por não serem fulcrados em leis igualitárias positivadas, que não raro beneficiavam a nobreza.

O período histórico sente uma mudança de conceituação em que o delito deixa de ser um ato que afronta os direitos da vítima e passa a ser um ato contra a paz da pessoa do monarca e, conseqüentemente, contra a sociedade em geral.

²³³ Os mesmos KEARON e GODFREY apontam que as fianças tornaram-se um a fonte crescente, pois lucrativa para o Estado vingativo que chegou a criar coletores de taxas itinerantes que serviam também como magistrados itinerantes, concentrando ambas funções. KEARON, Tony e GODFREY, Barry S.. *Setting the Scene: a question of history*. Handbook of victims and victimology. Willan Publishing. Londres. 2007. pp. 18-22. No mesmo sentido: STANGELAND, Per. *Criminología realista y El problema de las víctimas*, in Problemas criminológicos em las sociedades complejas (coordenadores: BIDASOLO, Mirentxu Corcoy e GARCÍA, Carmen Ruidiaz). Universidad Pública de Navarra. Espanha, 2000, p.131.

²³⁴ OLIVEIRA, Ana Sofia Schmidt de. Op. cit. p. 33.

A necessidade de criação de poderes com funções diferenciadas surge com o crescimento da participação do poder centralizado e, com a aplicação da jurisdição, surgem as formas de punição iníquas, violentas e desumanas. Beccaria, em seu livro conceitual, inaugura a fase de questionamento dos fins da pena, do processo legal e das provas utilizadas, num forte viés de avaliação do fenômeno crime, em detrimento de variáveis humanas²³⁵.

O passar da titularidade de resolução de conflitos para o Estado e seu questionamento, trouxeram conjuntamente ganho na criação de estudos e raciocínios focados no ato-crime num sentido kantiano, ou seja, estabelecendo-se valores pré-determinados pela legislação, que estabelece os bens jurídicos a serem primacialmente tutelados. Por conta disso, passou-se a ideia de que o cometedor de um fato típico, previsto na legislação como delito, responderia pela atitude num raciocínio *ex post*, e que privilegiava o resultado.

Assim, construído estava o raciocínio da teoria causalista em que o desvalor do resultado é o principal parâmetro de prejuízo a ser coibido pelo Direito Penal e pelo Estado, e em que o esforço primordial estava no raciocínio de se construir a relação ou nexos entre a ação de um indivíduo e o resultado obtido. Deixa-se de lado o estudo do subjetivismo dos atores do fato em prol da objetividade da lesão analisada, porém, após o cometimento do fato. O custo é que a vítima, *a fortiori*, desaparece do raciocínio penal (“*evaporación vitimal*”)²³⁶ por conta de sua irrelevância no raciocínio jurídico proposto.

A partir do iluminismo e com o regresso da permissividade para que as ciências fossem (voltassem a ser) desenvolvidas, que cientistas fazem com que o Direito passe a focar o delinquente como mote primordial de estudo, aumentando para duas as importâncias no estudo da delinquência e gerando as raízes de uma teoria finalista. Intenção e vontade do agente passam a ser valores a serem considerados – e por vezes até mesmo descartados a partir de estudos empíricos –, aumentando-se para além do desvalor do resultado, o conceito de desvalor da ação (ou desvalor da intenção²³⁷), que por si recebe maiores preocupações.

²³⁵ BECCARIA, Cesare. Dos Delitos e das Penas. Editora Martins Fontes, São Paulo, 2005, *passim*.

²³⁶ MORENO, Myriam Herrera. Sobre los Orígenes Científicos de La Victimología. *Cuadernos de política criminal*, n. 56. Editoriales de Derecho Reunidas, S.A., Madrid, 1995, p.482.

²³⁷ Segundo Luis Greco in Um Panorama da Teoria da Imputação Objetiva. Lumen Juris Editora, Rio de Janeiro, 2005, p. 11.

Contudo, a vítima ainda não recebe o devido cuidado, e os olhos do pensador penal prestam atenção superior e especial ao delinqüente e sua subjetividade.

Como explanado supra, somente no final da década de 40 chama-se a atenção para a importância de também se considerar a vítima como fundamental na compreensão e repressão da delinqüência, compondo amplamente a ecologia do delito.

O Primeiro Simpósio de Vitimologia ocorreu somente em 1973, em Jerusalém, e discutiu o tema, propondo que o fato criminoso fosse estudado não só restrito à figura do delinqüente, mas também a partir de uma perspectiva da vítima e sua relação com o delinqüente, pois que a diminuta atenção ao lesado fadaria o Direito Penal ao fracasso²³⁸.

A proposta de se voltar os olhares também ao ofendido direto gerou diferentes aspectos, pois que diferentes perspectivas existem ao se buscar o estudo científico das vítimas do delito ou a partir de sua perspectiva.

Certamente que diversos questionamentos como o do esquecimento da vítima e sua relegação para segundo plano quanto ao cuidado e à reparação de seu dano em sentido amplo sofrido – a si e à sua família e dependentes – e, por conseguinte, as criações de bens jurídicos difusos e coletivos, demonstrou que também ofendidos indiretos abarcariam um conceito de vítima. E esse fato as legislações deixaram de fora, como também o tratamento das vítimas por parte das autoridades e o estímulo à denúncia dos fatos.

Importante notar que a consolidação das teorias funcionalistas, em especial da imputação objetiva também prestaram auxílio fundamental para o surgimento do enfoque vitimal. Isso porque, nas palavras de Cancio Meliá:

“A teoria da imputação objetiva, então, vem a reformular a tipicidade objetiva. A partir dessa perspectiva, implica a introdução de elementos valorativos que determinam quais são os limites da liberdade de atuação, o que implica, nesse sentido, o estabelecimento de esferas de responsabilidade. Um dos setores em

²³⁸ ARUS, Francisco Bueno. “La atención a La víctima del delito”. *Actualidad Penal*. Actualidad Editorial S.A., Madrid, 1990. pp. 297-298.

*que a imputação objetiva pode ser o marco sistemático adequado é o relativo à questão dos âmbitos de responsabilidade nos casos em que concorre na gênese de um risco a pessoa que posteriormente resulta lesionada.*²³⁹”

Contudo e inicialmente, é necessário compreender-se que o mote deste trabalho está na vítima direta, daquela que mantém algum contato com o ofensor. Busca-se considerar a relação entre aquele que é vítima de uma conduta e aquele que faz alguém ser vítima, denominado vitimário. A esta relação, deu-se o nome de “*parelha penal*”, ou seja, a ligação existente entre a vítima e seu vitimário e que por vezes influi no acontecimento do delito. Nas palavras de Elías Neuman:

*“A ‘parelha penal’ não é nada harmônica, senão contraposta. Em algum caso pode começar sendo harmônica – como no estelionato –, mas o que interessa ao delinquente, seu desejo íntimo porque dali resultará seu êxito, é o de causar, ao final, essa desarmonia que determina e destaca os papéis que estavam destinados no ato delitual: vitimário e sacrificado. (...) O estudo das relações interpessoais implica um jogo de subjetivismos que interessa profundamente ao criminólogo.*²⁴⁰”

Ao se pensar em vitimologia, é imprescindível a compreensão de que existem diferentes momentos para que um delito ocorra e, pois, diferentes circunstâncias em que aquele que sofrerá diretamente o fato se encontra, bem como aquele em que o praticará.

Diz-se que existe o momento anterior à prática criminal, existe o momento da prática criminal em si e existe o momento posterior ao fato. No momento anterior, ambos indivíduos estão numa situação normal, em que ainda não assumiram nenhum papel: o futuro vitimário

²³⁹ CANCIO MELIÁ, Manuel. La exclusión de la tipicidad por la responsabilidad de La víctima (“imputación a la víctima”). *Direito e Democracia – Revista de Ciências Jurídicas* v. 6, n. 2 – 2º semestre de 2005, Editora ULBRA, 2005, p. 465.

²⁴⁰ “La ‘pareja penal’ no es en nada armónica sino contrapuesta. En algún caso puede comenzar siendo armónica – como en la estafa -, pero lo que interesa al delincuente, su deseo íntimo porque de ahí resultará su êxito, es el de causar, al final, esa desarmonia que determina y destaca los roles a que estaban destinados en El acto delictual: victimario y sacrificado. (...) El estudio de las relaciones interpersonales implica un juego de subjetivismos que interesa profundamente al criminólogo” NEUMAN, Elías. Op. cit. pp. 35-36.

está maturando as ideias de cometimento do fato (fase interna – cogitação, ponderação, resolução – e fase externa - preparação) e a futura vítima está em situação de fragilidade ou vulnerabilidade.

No momento do acontecimento do delito, o vitimário já se encontra em execução. Dependendo do tipo de delito, a vítima poderá compreender que está numa situação de vitimização e preparar-se para defender-se, caso seja possível.

Ocorrido o fato sem que a vítima tenha podido ou conseguido se defender²⁴¹, está-se diante do momento de consumação do tipo penal. Fica consolidado o papel de cada um dos atores, vítima e vitimário e surge consolidado o delito.

Edmundo Oliveira apresenta a ideia de que se poderia falar de um verdadeiro *iter victimae* em que 4 fases são apontadas²⁴²:

À primeira fase denominou o autor “intuição”, em que a vítima pode ter a ideia, ou faz nascer a previsibilidade de poder ser alvo de um ofensor. É uma fase assemelhada à expectativa, em que conhecendo a si, a situação em que se encontra e o ambiente, nota que poderia ser escolhida como objetivo.

Em seguida, a vítima passa a preparar seu comportamento defensivamente, consensualmente ou conforma-se que será ofendida: É a segunda fase, preparatória.

A terceira fase vitimal (pré-execução) relaciona-se com o início da execução por parte do agente e a vítima inicia sua defesa efetivamente, ou coopera, apoia ou facilita a comissão ou omissão do ofensor. É apenas a fase em que os atos de reação ou não reação se iniciam, pois a fase seguinte (quarta fase) é denominada de execução em que a vítima efetiva sua resistência de modo absoluto ou deixa-se vitimizar.

Para o autor, duas são as possibilidades quanto à vítima resistente: haver a consumação ou meramente a tentativa do fato, sem atingimento dos objetivos, porquanto a reação vitimal

²⁴¹ Caso a defesa fosse profícua, estaríamos diante de um crime tentado, em que o vitimário não teria obtido resultado pretendido por circunstância alheia a sua vontade, por reação de uma vítima tentada. A proposta de um *iter victimae* pode ser observada nos escritos de Luiz Rodríguez Manzanera in *Victimologia: estudio de la víctima*. Porrúa, Mexico, 1990, p. 142.

²⁴² OLIVEIRA, Edmundo. Novos rumos da vitimologia - O crime precipitado pela vítima. *Boletim Instituto*

será suficiente para evitar a consumação. No que se refere à vítima cooperante ou pacífica, certamente só haverá tentativa se a circunstância alheia à vontade do vitimário for de terceiro, tendo-se em vista que o lesado aceitou ou agiu conforme o intuito de consumação.

Há total relação entre as fases do *iter criminis* e as do *iter victimae*: aos atos internos (cogitação, ponderação e resolução) haveria correspondência com a fase intuitiva; aos atos preparatórios do autor, a fase de mesmo nome da vítima; à fase executória, as fases de início de execução e execução da vítima; finalmente, à consumação do delito ou à tentativa, no exaurimento da conduta do agente, estão as fases de mesmo nome para a vítima.

Com isso é interessante notar-se que a estrutura do crime pode sim ser analisada em aspectos semelhantes no que se refere a ambos os sujeitos.

A estrutura do delito admite a existência de um ou mais sujeitos praticantes – denominados autor ou, para alguns, sujeito ativo – e, em contraposição ao autor, há a figura da vítima ou as vítimas – pessoas físicas, jurídicas ou ideal (sociedade, coletividade) que sofre os efeitos diretos da atitude dita criminosa, por alguns chamada de sujeito passivo.

Há que se destacar que vítima de crime não pode ser confundida com objeto jurídico ou objeto material, estes específicos de condutas concretamente analisadas, e aquele se referindo ao conceito de bem jurídico. Uma pessoa pode ser vítima de dois furtos, entretanto cada qual terá um objeto material diferente (uma carteira e um computador, p. ex.), mas em ambos os casos é o patrimônio em sentido amplo o objeto jurídico violado.

Foi o estudo particular de cada um dos sujeitos do crime que levou a ciência a desenvolver braços da criminologia como a psiquiatria do criminoso, a psicologia da conduta criminosa e outras ciências dedicadas ao praticante do fato lesionador.

Na mesma toada veio a vitimologia como ramo da criminologia, em que interessa mais acentuadamente o comportamento da vítima diante de um delito (visto que inserida no mesmo ambiente social de risco que o agente), além de sua reação defensiva, a comunicação da lesão, sua fragilidade, a necessidade de sua reparação, etc.

A expressão vítima merece detalhada observação, em especial quanto ao seu significado e as classificações apresentadas.

As raízes da expressão remontam ideias antepassadas em que vítima era a pessoa ou animal sacrificado em homenagem a uma divindade. Também, o dicionário denomina vítima aquela pessoa que é morta por outrem, sacrificada ou passiva numa ação, sofrendo danos e prejuízos²⁴³.

De acordo com Frederico Abrahão de Oliveira, vítima seria “*pessoa que sofre danos de ordem física, mental e econômica, bem como quem perde direitos fundamentais, seja em razão de violações de direitos humanos, bem como atos de criminosos comuns*”²⁴⁴. Alessandra Orcesi Greco²⁴⁵, por sua vez, define vítima como sendo “*a pessoa, física ou jurídica, que sofre uma lesão ou uma ameaça de lesão a seu bem jurídico*” e também, de modo mais abrangente “*aquele que sofre as consequências de determinada conduta típica, de modo relevante, que propicia a atuação do Estado para atingir os fins do Direito Penal, no Estado Democrático de Direito*”²⁴⁶.

Porém, a melhor definição advém da resolução 40/34 de 29.11.85, da Assembleia Geral das Nações Unidas²⁴⁷, aponta que internacionalmente a definição de vítima é:

“Pessoa que, individual ou coletivamente, tenha sofrido danos, inclusive lesões físicas ou mentais, sofrimento emocional, perda financeira ou diminuição substancial de seus direitos fundamentais, como consequências de ações ou omissões que violem a legislação penal vigente, nos Estados – Membros, incluída a que prescreve o

²⁴³ Dicionário Eletrônico Michaelis. Disponível em <http://michaelis.uol.com.br/moderno/portugues/index.php?palavra=v%EDtima>. Acesso em 14.01.09 às 15:24hs.

²⁴⁴ Apud OLIVEIRA, Ana Sofia Schmidt de. Op. cit. p. 78.

²⁴⁵ GRECO, Alessandra Orcesi Pedro, “A autocolocação da vítima em risco”, Editora Revista dos Tribunais, São Paulo, 2004, p. 23.

²⁴⁶ No mesmo sentido mais amplo ver Antonio Beristain em seu artigo “Desde la Victimología de Mínimos hacia La Victimología de Máximos” in Cuadernos de Política Criminal, nº 85. Edita Centro de Estudios Superiores de Especialidades Jurídicas, Espanha, 2005, pp. 255-258.

²⁴⁷ “‘Victims’ means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power.” Disponível em <http://www2.ohchr.org/english/law/victims.htm>. Acesso em 06.01.08 às 15:11hs.

abuso de poder”

No entanto, especialmente ao levar-se em conta o tema aqui tratado, qual seja, a criminalidade informática, uma série de dificuldades em assumir qualquer das definições acima apresentadas surge.

Isso se dá, por exemplo, na hipótese de se concentrar o estudo nos crimes denominados informáticos próprios puros, pelo fato de sua existência demandar a concepção de novos bens jurídicos, novas valorações e novos Principios, nenhum deles ainda devidamente admitido pela doutrina brasileira. Com isso, fica imediatamente a definição de vítima por desatendimento à parte final da definição.

Ao se partir do pressuposto de que a vítima do crime informático é alguém que sofre as consequências de uma conduta típica, conclui-se que condutas lesionadoras que afetam bens jurídicos mas não têm tipo respectivo, não geram vítimas, o que gera uma contradição e uma sensação de inquietude.

Há, ainda, que se apresentar o fato de que delitos informáticos podem não gerar danos patrimoniais, físicos ou econômicos, limitando-se a questões morais ou até mesmo meras violações de sigilo sem qualquer repercussão em outra esfera.

Por isso opta-se inicialmente pela definição mais abrangente, qual seja a internacional, em que se considera que dano de ordem emocional ou meras reduções de direitos podem ser consideradas violações geradoras de vítimas, com a ressalva novamente de que se mantém o raciocínio dogmático penal (Princípio da legalidade) dentro de uma concepção que busca ser criminológica.

Alguns estudos tipológicos, por exemplo, negam que a vitimologia restrinja seus aspectos de pesquisa nas vítimas em sentido legalista, ou seja, a vítima como sendo somente o alvo direto ou indireto de uma ação típica. Deste modo, é crescente a aceitação de que o objeto da vitimologia não está adstrito às vítimas dos delitos, podendo-se estender a concepção para demais pessoas envolvidas em um processo vitimizatório. Assim posiciona-se Ana Isabel Garita Vilchez que acrescenta a ideia de que pode ser vítima a pessoa que sofreu alguma violação de Principios de direitos humanos e, ainda, pessoas que estão envolvidas em abusos

de poder²⁴⁸.

Também neste jaez doutrinadores acerca da tipologia ampla quando consideram que vítimas podem ser classificadas como sendo a) vítimas de nascimento; b) vítimas dos pais; c) vítimas da civilização; d) vítimas do Estado e e) vítimas da tecnologia, conforme proposto por Vasile Stanciu²⁴⁹; Eliás Neuman, por sua vez, acrescenta a modalidade da “vítima da sociedade e do sistema social”²⁵⁰.

Resta uma concepção refletida de que vítimas são pessoas físicas ou jurídicas que sofrem lesões direta ou indiretamente através de atos humanos ou fatos naturais e que por conta desse acontecimento sofrem consequências lesivas a direitos, bens jurídicos ou até mesmo a Princípios, não se exigindo necessariamente que o ato desencadeador de prejuízos de qualquer ordem sejam tipificados na positivação penal. Existem, pois, vítimas sem que haja crimes como nos clássicos exemplos da autolesão ou da catástrofe natural.

Ainda no que concerne à vítima e suas modalidades, é importante que antes de apresentar outras tipologias classificatórias, determine-se o âmbito de atuação dessa ciência.

Para Mendelsohn, há uma questão subjacente a ser considerada pois vitimologia é o estudo da personalidade da vítima que foi lesionada por um delinquente ou por outros fatores, como consequência de uma inclinação subconsciente. Também interessante apontamento do objeto da vitimologia é de Gugliermo Gulotta²⁵¹ que determina que é ciência que estuda a vítima, sua personalidade, suas características, suas relações com o delinquente e o papel que assumiu na gênese do delito.

Entretanto, preferiu-se os objetos apresentados minuciosamente por Lola Anyiar de

²⁴⁸ “El Sistema de Justicia Penal desde La Perspectiva Vitimológica”. Conferência proferida no Seminário preparatório ao VII Simpósio Internacional de Vitimologia, Rio de Janeiro, 1991. Também em http://www.inecip.org/cdoc/reforma_de_la_justicia_penal/jusrestaurativa.pdf. Acesso em 14.01.09 às 16:28hs.

²⁴⁹ STANCIU, Vasile V. *Les Droits de La Victime*, Presses Universitaires de France, France, 1985, pp. 45 e ss. *apud* PIEDADE JUNIOR, Heitor. *Vitimologia*. Livraria Freitas Bastos S.A.. 1993. Rio de Janeiro. p. 103. Também, MOREIRA FILHO, Guaracy. *Vitimologia – O papel da Vítima na Gênese do Delito*. Editora Jurídica Brasileira, São Paulo, 1999, p. 48.

²⁵⁰ NEUMAN, Elías. *Op. cit.* pp. 56-59.

²⁵¹ GULOTTA, Gugliermo. *La Vittima*. Giuffrè Editore. Itália. 1976, p. 9 *apud* PIEDADE JÚNIOR, Heitor. *Op. cit.*, p. 82. Também, MOREIRA FILHO, Guaracy. *Vitimologia – O papel da Vítima na Gênese do Delito*. Editora Jurídica Brasileira, São Paulo, 1999, p. 47-48.

Castro que sintetiza os espectros da vitimologia²⁵² como sendo, em linhas gerais:

- 1- Estudo da personalidade da vítima como consequência de suas inclinações subconscientes;
- 2- Descobrimiento dos elementos psíquicos que determina a aproximação entre a vítima e o criminoso;
- 3- Análise da personalidade das vítimas sem intervenção de um terceiro;
- 4- Estudo dos meios de identificação dos indivíduos com tendência a se tornarem vítimas.
- 5- Busca dos meios de prevenir a recidiva da vítima.

O estudo em tela trata especificamente da preocupação com o enfoque detido da ação da vítima e as consequências desta com a delinquência, partindo-se do pressuposto de que a forma de um individuo se comportar tem forte influência no cometimento de um crime. É, pois resumidamente o estudo da aptidão e tendência de alguém a tornar-se vítima.

A partir dos objetos apresentados como alvo do estudo da vitimodogmática, fundamental que se apresente a diferenciação entre vítima e sujeito passivo, de grande importância para as próximas linhas.

O Direito Penal criou a expressão “sujeito passivo” – que mormente não se encontra em qualquer lei penal como expressão legal²⁵³ – no intuito de relacionar e contrapor as ideias de que o delito é um fenômeno dúplice: de um lado há um ou mais agentes responsáveis pela violação do bem jurídico através de uma ação, e de outro lado há uma ou mais pessoas que sofrem as consequências da ação.

Tal forma de o Direito Penal interpretar o fenômeno delituoso faz com que a

²⁵² ANIYAR DE CASTRO, Lola. *Victimología*. Univerisdade Del Zulia, Venezuela, 1969, p. 27.

²⁵³ Conforme Guaracy Moreira Filho, as terminologias encontradas, especialmente nos Códigos Penal e de Processo Penal são “ofendido”, “lesado” e “vítima”. Vide artigos 5º, 6º, 14, 19, 24, 30, 31, 32, 33, 34, 38, 39, 45, 50, 63, 119, 122, 127, 133, 134, 140, 142, 188, 201, 229, 240, 268, 458, 526, 529 e 598 do CPP e artigos 20, 59, 61, 65, 71, 94, 100, 103, 104, 105, 106, 107, 121, 122, 129, 133, 138, 139, 140, 144, 145, 148, 157, 160, 163, 216, 221, 224, 225, 226, 227 e 240 do CP. MOREIRA FILHO, Guaracy. *Vitimologia – O papel da Vítima na Gênese do Delito*. Editora Jurídica Brasileira, São Paulo, 1999, p. 51-64.

concepção de vítima tome um vulto de fragilidade e suscetibilidade, rechaçado pela sociedade. Por sua vez, a figura do delinquente passa a ser vista como forte e ameaçadora enquanto que a do lesado é vista como fraca e débil. Preocupa-se o Direito Penal – e o poder legislativo – com o estudo de uma vítima que pode ser classificada como pura: a viúva vulnerável, a pessoa de idade medrosa, o órfão abandonado, a mulher honesta, o adolescente vulnerável, o empregado dependente e assim por diante.

Tal perspectiva faz com que se gere uma gama de consequências nos indivíduos: consegue o indivíduo comum colocar-se na posição de delinquente, mas não consegue (por não querer) colocar-se na posição de vítima; a vítima fica estigmatizada como um sujeito fracassado; o foco acerca da repreensão concentra-se na figura do delinquente e até mesmo descarta-se a ideia de que pode haver vítimas sem que haja um sujeito ofensor. Nas palavras de Guilherme Costa Câmara:

*“Ainda há que se incluir um outro componente para a sublinhada colatização da vítima do discurso punitivo, este de tonalidade psicológica: as pessoas tendem a identificarem-se menos com a vítima (vista muitas vezes como perdedora), do que com o delinquente.”*²⁵⁴

Porém, ao se observar a vítima a partir dos aspectos acima apontados, a realidade mostra-se diversa em muitos casos. Diversos tipos penais admitem que a vítima possa ter participação ativa no cometimento do fato, porquanto pode agir de modo provocativo, ser desidiosa quanto aos seus deveres de cuidado, contribuir para o acontecimento lesivo e até mesmo confundir-se com a figura do lesionador²⁵⁵.

Ao pensar em vítima como sujeito amplo que sofre consequências de atos até mesmo de desigualdade social, preconceito a partir de sua cor de pele e até mesmo *bypassers* de atos terroristas ou organizações criminosas, fala-se de figuras que nada têm a ser considerado por serem alvos de infortúnios. Fazem parte de uma macrovitimização ou de uma vitimização

²⁵⁴ CÂMARA, Guilherme Costa. Op. cit. p. 49.

²⁵⁵ Exemplo nesse sentido são o homicídio praticado após injusta provocação da vítima (art. 121, §1º, CP) e os crimes de auto-acusação falsa (art. 341, CP).

difusa²⁵⁶. Contudo, suicidas são vítimas de seus próprios atos, assim como, do mesmo modo, usuarios de entorpecentes.

Importante apresentar aqui, então, o necessário posicionamento avesso à expressão “*sujeito passivo*”, utilizada pela doutrina penal. Concorde-se com Manuel Cancio Meliá quando diz, ao refletir a vitimodogmática, haver que se considerar necessariamente a influência da vítima na criação do risco relevante para o Direito Penal²⁵⁷; assim, o termo “*sujeito passivo*” leva a uma sugestão de inércia por parte daquele que suporta a conduta criminosa do autor, o que, segundo a vitimodogmática, é inaceitável vez que a vítima interage com o agente e com o meio e tais dados devem ser levados em conta para uma correta apreciação fática.

O conceito de sociedade de riscos e de previsibilidade decorrente de tais riscos, portanto, aplica-se a todos os sujeitos, seja àqueles que os criam, seja àqueles que os sofrem. Visto que a recomendação legal positivada é a de que os primeiros não criem lesões a direitos (e no caso de tipos penais abstratos, não criem o risco de criarem lesões), é de se presumir, também, que haja uma recomendação também no sentido de que os segundos não facilitem a criação de riscos pelos primeiros. Diante disso surge a idéia da existência de Principios vitimológicos em que se aceita a competência da vítima e sua auto-responsabilidade de evitação de certas situações, conjuntamente com o surgir da concepção de um verdadeiro processo de vitimização que inclui “desde o atuar inconsciente da vítima até seu agir deliberado fundindo-se aos propósitos do vitimizador”, nas palavras de Heitor Piedade Junior²⁵⁸.

Pensando em tais possibilidades, outras tipologias vitimais surgiram, após influência da própria tipologia do delinquente.

Tendo-se em vista a importância da análise tipológica para analisar os tipos mais comuns de delitos informáticos a serem tratados, algumas linhas àquelas tipologias serão

²⁵⁶ CÂMARA, Guilherme Costa. Programa de Política Criminal Orientado para a Vítima do Crime. Co-edição Coimbra Editora e Editora Revista dos Tribunais, São Paulo, 2008, p. 13.

²⁵⁷ Cancio Meliá, Manuel. *Conducta de la víctima e imputación objetiva em Direito Penal*. Barcelona: Bosch, 1998, *passim*.

²⁵⁸ PIEDADE JUNIOR, Heitor. Op. cit., p. 115. Também nesse sentido, OLIVEIRA, Ana Sofia Schmidt de. Op. cit. pp. 110-117.

apresentadas por parecerem interessantes para o estudo em tela.

Mendelsohn propôs que se graduasse através de porcentagens a quantidade de participação que uma vítima teria no delito, e informava que poderiam existir: a) vítimas ideais ou completamente inocentes; b) vítimas por ignorância ou menos culpadas que o delinquente; c) vítimas provocadoras ou tão culpadas quanto o delinquente; d) pseudovítimas ou vítimas mais culpadas do que o delinquente; e e) vítimas agressoras ou unicamente culpadas. Seriam, em decorrência disso, três os grupos de vítimas: 1- o de vítimas inocentes, sem qualquer participação no resultado, 2- o de vítimas provocadoras, imprudentes, voluntárias ou ignorantes com participação certa do fato, e 3- vítimas agressoras, simuladoras e imaginárias, verdadeiras co-autoras do delito.

Von Hentig aprontou uma classificação que levava em conta o interesse da vítima em participar do delito, dividindo-as em resistentes ou coadjuvantes²⁵⁹. Jimenez de Asúa, diversamente, enfoca uma classificação pelo objetivo do delinquente, dividindo as vítimas em 1- indiferentes, 2- indefinidas ou inominadas e 3- determinadas²⁶⁰.

Apontado por Heitor Piedade Júnior, a classificação de Marwin Wolfgang é a de que as espécies são: a) vitimização primária que leva em conta a personificação da vítima ou sua individualização; b) vitimização secundária que enfoca a impessoalidade da vítima, sua comercialidade e sua abrangência coletiva, mas não difusa; c) vitimização terciária que seria o ataque difuso que se estende a toda a comunidade; e d) a vitimização mútua em que há consensualidade entre participantes para a prática²⁶¹. Exemplo da primeira classificação seria a extorsão mediante sequestro de um artista de televisão, no segundo caso, o roubo de um banco e, no terceiro caso, um crime contra o meio ambiente.

Ezzat Fattah também apresenta uma classificação relevante. Desdobra em vítimas sem qualquer responsabilidade e vítimas com responsabilidade. Aquelas com responsabilidade, por sua vez, subdividem-se em a) vítimas desejosas ou suplicantes, que esgota esforços ativos para permitir que o processo vitimizador se complete; b) vítimas de consentimento livre, que não

²⁵⁹ VON HENTIG, Hans. *The Criminal & His Victims – Studies in the Sociobiology of Crime*. Yale University Press, New Haven, 1948, pp. 383-450.

²⁶⁰ NEUMAN, Elías. Op. cit. pp. 51-52.

²⁶¹ WOLFGANG, Marvin E. *Studies in Homicide*. Harper and Row, New York, 1967, pp. 72-88 *apud*

vai de encontro com a prática cooperando mas sim não resiste, não objeta nem impede o acontecimento; e c) vítimas que devem ser responsabilizadas mesmo não consentindo no processo de vitimização por conta de terem propiciado o resultado. É também de Fattah a classificação em que divide a vítima em a) não participante; b) latente ou predisposta; c) provocativa; d) participante; e e) falsa²⁶².

Uma classificação mais abrangente é aquela que leva em conta ser a vítima a) individual, b) familiar, c) coletiva, d) da sociedade e do sistema social, apresentada por Neuman, levando em conta a ideia de que, em alguns casos, a vítima assim nasce pelo fatídico destino da posição social, família e das desigualdades existentes²⁶³.

Finalmente é de se apresentar a classificação de Lola Aniyar de Castro que divide as vítimas em agrupamentos, sendo a) vítima singular e coletiva; b) vítima de si mesma e vítima de crimes alheios; c) vítima por tendência, reincidente, habitual e vítima profissional; e d) vítima com culpa inconsciente, vítima com culpa consciente e vítima com dolo²⁶⁴. Esta classificação é múltipla e envolve diversos aspectos que podem coexistir numa situação concreta. Assim, uma vítima que sofre um furto por utilizar o celular em local perigoso seria simultaneamente singular, vítima de si mesma, vítima por tendência e vítima com culpa consciente, exemplificativamente.

Desta forma, as diferentes tipologias apresentadas podem levar em conta os seguintes aspectos: (i) a escolha do criminoso, (ii) a capacidade de a vítima impedir o resultado, (iii) a quantidade de participação da vítima, (iv) a imersão social da vítima, (v) a criação da vítima, (vi) a abrangência da vitimização, (vii) a proximidade da vítima com o delinquente e (viii) a responsabilidade da vítima com o fato.

Tais diferentes nuances relativas às vítimas fazem com que seja importante, neste ponto, explanar-se a expressão “vitimidogmática”. Nas palavras de Margarita Bonet Esteva, seria:

PIEADADE JUNIOR, Heitor. Op. cit. p. 84.

²⁶² PIEADADE JR., Heitor. op. cit. p. 155.

²⁶³ NEUMAN, Elías. Victimologia. Editorial Universidad. Buenos Aires. 1994. pp. 56-59.

²⁶⁴ ANYIAR DE CASTRO, Lola. Victimología. Universidad Del Zulia, Venezuela, 1969, p. 76 *apud* PIEADADE JUNIOR, Heitor. Op. cit. p. 104. Também, MOREIRA FILHO, Guaracy. Vitimologia – O papel da Vítima na Gênese do Delito. Editora Jurídica Brasileira, São Paulo, 1999, p. 49.

*“(...) aquele conjunto de correntes teóricas que reinterpretem em certo sentido a dogmática jurídoc-penal à luz dos Principios vitimológicos”*²⁶⁵

Quatro são os principais Principios vitimológicos: o da subsidiariedade, o da fragmentariedade, o da proporcionalidade e o da auto-responsabilidade (ou da autocolocação em risco).

No primeiro caso, está-se tratando da *ultima ratio* propriamente dita, mas num enfoque em que se leva em conta a ação estatal quando da inação da vítima ou, ainda, a ideia de que certos bens jurídicos só devem ser defendidos oficialmente pelo direito após a manifestação do lesado nesse sentido, num diagnóstico de necessidade de proteção²⁶⁶. É um Principio que tem vigência na doutrina pátria, especialmente se levar em conta o conceito das figuras da ação penal privada e mesmo de ação penal pública condicionada. Na primeira, exige-se que a iniciativa particular promova a petição inicial do processo penal para somente a partir disso inicie-se uma possível persecução penal, privilegiando-se o interesse da vítima quanto ao bem jurídico exclusivo violado. Na segunda, ainda que o impulso processual seja oficial, há o condicionamento para um determinado ato denominado representação criminal em que a vítima deve manifestar interesse em processar criminalmente seu ofensor, protegendo bens jurídicos importantes, mas com preponderante valor ao lesionado.

Ainda norteados pelas ideias da subsidiariedade, alguns pensadores entendem que a busca do Direito Penal deveria ser, em muitos casos, por meios alternativos de satisfação e reparação da lesão.

O Principio da fragmentariedade complementa a ideia de subsidiariedade no sentido dimensional. Para que a ciência penal possa ser subsidiária das demais, é de se entender que esta compõe apenas uma parcela do direito dedicado à tutela dos atos ilícitos. Ao Direito Penal

²⁶⁵ “(...) aquel conjunto de corrientes teóricas que reinterpretan em cierto sentido La dogmática jurídico-penal a La luz de Principios victimológicos.” ESTEVA, Margarita Bonet. La Víctima Del delito (La autopuesta em perigo como causa de exclusion Del tipo de injusto). McGraw Hill. Madrid. 1999. p. 63.

²⁶⁶ Nas palavras de SCHÜNEMANN, “La imposicion de La pena como ultima ratio del Estado no ES apropiada em aquellos casos em los que La víctima no merece protección” e que se deve “eliminarse Del âmbito de lo punible (...) todas aquellas formas de comportamiento (...) frente a las cuales La víctima puede protegerse a sí misma de modo sencillo y exigible sin más”. CANCIO MELIÁ, Manuel. Op. cit. p. 474.

sobejam as condutas de máximo gravame geradoras de insegurança social²⁶⁷. Por Muñoz Conde, três são os aspectos a serem levados em conta no que se refere a tal característica do Direito Penal: a) o fato de que somente alguns bens jurídicos serão protegidos e somente por conta de alguns especiais modos de ataque excluindo-se a punibilidade em boa parte das ações culposas, b) incidindo somente em algumas condutas em consonância com outros ramos do Direito e c) deixando de lado ações imorais.²⁶⁸

O Princípio da proporcionalidade, pelo enfoque vitimodogmático, é aquele que aponta para o fato de que o Estado somente tutela penalmente os bens jurídicos quando sua violação é contrária aos fins almejados pelo ordenamento jurídico. Desta forma, bens jurídicos disponíveis têm sua titularidade protetiva nos próprios interessados, indivíduos particulares, que livremente podem renunciar à sua proteção jurídico-penal²⁶⁹. Por isso, seria desproporcional que o Direito Penal se importasse com condutas que renunciam legitimamente sua atuação, especialmente frente a algumas condutas tácitas ou expressas de vítimas, conforme se verá adiante.

No que se refere à autocolocação, dedicar-se-á momento específico para tratá-la, contrapondo-a com a ideia de consentimento do ofendido.

Por hora, o que nos importa é a visualização de que norteados pelo foco vitimal (permeado certamente pelos Princípios da vitimologia) diversos aspectos se mostram relevantes no estudo vitimodogmático, aqui condensados por Francisco Buenos Arus:

“(...) incumbe à vitimologia cobrir espaços teóricos-empíricos impolicados com a descrição da interação delinquente-vítima e sãs cambiantes projeções, com o conjunto de atitudes e reações determinantes da vítima, sua vulnerabilidade, seleção, aumento dos riscos, bem como, com o fenômeno da vitimização difusa e indiscriminada,

²⁶⁷ NUCCI, Guilherme de Souza. Manual de Direito Penal. 3ª Edição. Editora Revista dos Tribunais. São Paulo. 2007. p. 71.

²⁶⁸ MUÑOZ CONDE, Francisco. Introducción al Derecho Penal. Bosch. Barcelona. 1975, *apud* BITENCOURT, Cezar Roberto. Tratado de Direito Penal. Parte Geral. 10ª. Edição. Editora Saraiva. 2006. p. 19.

²⁶⁹ MALANDA, Sergio Romeo. La Relevancia Jurídico-Penal de La Conduta de La VíCtima em los Delitos de Estafa. In Hanz Welzel em El Pensamiento Penal de La Modernidad (Diretores: Hans Joachim Hirsch, José C

com especial ênfase na prevenção de todas as formas de vitimização criminal e na reparação dos danos”²⁷⁰

Abordaremos especialmente algumas tendências de vitimização, sob aspecto da perigosidade e da receptividade e possibilidade de prevenção da gênese delinquente sob enfoque da vítima. Isso porque é interesse da vitimodogmática a valoração normativa do comportamento do autor sob a ótica da vítima, visto que sua figura pode modificar a forma como a aplicação do direito penal ocorrerá no caso concreto²⁷¹.

Destaque-se somente, que para os fins deste trabalho, a forma como há o sofrimento do fato, a sugestibilidade, a influência que sofre e as ações da vítima não podem ser consideradas em níveis de ações difusas, uma vez que os crimes que atingem bens difusos (erroneamente denominados por alguns de crimes sem vítimas) não pressupõem qualquer reação de interação sendo, pois, delito unilateral e aqui atem-se à microvitimização exclusivamente.

Por isso, ao focar-se o estudo dos crimes informáticos a partir de uma perspectiva vitimal, tem-se que avaliar diversos aspectos, dentre eles o fato de que nem sempre se pode pressupor que uma vítima é inofensiva e obediente, contrariando a ideia de que alvos de tipos penais são estáticos e acrescentando ideias como a de cooperação, negligência e até mesmo dolo.

É imprescindível que se compreenda que as considerações aqui trazidas restringem-se às situações em que a vítima informática é individual e há a possibilidade individual de proteção dos bens jurídicos²⁷². Portanto, ainda que se considere a expressão vítima em sentido amplíssimo nas linhas acima, e ainda que se entenda que a rede mundial de computadores seja um meio ambiente, as considerações que dizem respeito a detalhes comportamentais exigem que seja possível a avaliação hipotética considerada a partir de situações individualizáveis.

Os seguintes elementos devem ser apreciados para uma correta compreensão da

Mir e Edgardo Donna). Rubinzal-Culzoni Editores, Buenos Aires, 2005, p. 706.

²⁷⁰ BUENOS ARUS, Francismo. La posición de la Víctima em El Moderno Sistema Penal, BFD, n. 70, 1994, p. 369 *apud* CÂMARA, Guilherme Costa. Op. cit. p. 75.

²⁷¹ CANCIO MELIÁ, Manuel. La exclusión de la tipicidad por la responsabilidad de La víctima (“imputación a la víctima”). *Direito e Democracia – Revista de Ciências Jurídicas* v. 6, n. 2 – 2º semestre de 2005, Editora ULBRA, 2005, p. 452.

²⁷² HASSEMER, Winfried. *Introdução aos Fundamentos do Direito Penal*. Sergio Antonio Fabris Editor, Porto Alegre, 2005, p. 123.

vitimologia em seu braço vitimodogmático: a parelha vítima-vitimário (a relação entre ambos), a precipitação vitimal (por nós compreendida como a somatória da periculosidade vitimal - o comportamento exteriorizado do indivíduo que o torna um bom alvo de práticas – e a receptividade vitimal – as características internas dos indivíduos que o tornam subjetivamente mais suscetível à ser alvo) e a prevenção vitimal (a capacidade da vítima evitar um acontecimento danoso). Vejamos:

A PARELHA VITIMA-VITIMÁRIO

À relação entre a vítima e o delinquente denominou-se parelha penal ou parelha vítima-vitimário²⁷³. Para fins deste estudo, vitimário, será citado como sinônimo de delinquente, como aquele responsável por colocar (exclusivamente ou não) um indivíduo na condição de lesado.

Ao se tratar da relação entre vitimário e vítima, contudo, não se está pressupondo um cenário em que somente se analisa a ação do primeiro e o sofrimento (e até a reação) do segundo, mas sim um processo que se denomina vitimização²⁷⁴. Objetiva-se atingir a ideia de que tal processo é composto por todas as variáveis possíveis da ação dos indivíduos envolvidos na criação de uma situação de risco: tanto o delinquente quanto a vítima.

Por vezes o fato é gerado somente por ações do vitimário, como no caso de delitos de ação unilateral (delitos de intervenção)²⁷⁵ como é exemplo o crime de homicídio simples; por vezes a vítima e o vitimário participam da ação, relacionando-se e coadjuvando na ação, como

²⁷³ No caso, trata-se da parelha de relação para o cometimento do crime e não a relação desviante obtida, por exemplo, nos casos em que se verifica a Síndrome de Estocolmo em que, por exemplo, a vítima termina por tomar o lado do vitimário, cooperando no cometimento e manutenção do estado criminal, numa ação inimputável por existência de deturpação psicológica.

A parelha penal também foi denominada “parelha delinquente” por Escipión Sighele e “dupla-penal” por Mendelsohn. Reséctivamente NEUMAN, Elias. Op. cit. p. 35 e OLIVEIRA, Ana Sofia Schmidt. Op. cit. p. 95.

²⁷⁴ Mendelsohn também denomina “vitimidade” a relação entre vitimário e vítima, assim como Manuel Costa Andrade. ANDRADE, Manuel da Costa. A vítima e o problema criminal. Separata do volume XXI do Suplemento ao Boletim da Faculdade de Direito da Universidade de Coimbra. Coimbra Editora, Coimbra, 1980, p. 26 *apud* OLIVEIRA, Ana Sofia Schmidt de. Op. cit. p. 92.

²⁷⁵ Note-se, ao ler as principais doutrinas brasileiras, que praticamente nenhuma classificação dos crimes leva em conta o papel da vítima no ato. As principais classificações que encontramos são: a) crimes unissubjetivos ou plurissubjetivos; b) crimes unissubsistentes e plurissubsistentes; c) crimes de dano ou de perigo; d) crimes instantâneos ou crimes permanentes; e) crimes materiais ou crimes formais; f) crimes próprios e crimes

no estelionato; e por vezes, a ação é exclusivamente da própria vítima como no caso do uso de entorpecentes até a overdose.

Com isso, importante entender que as figuras de vitimário e vítima não podem ser conceituadas como necessariamente antagônicas, num pressuposto em que nem todo vitimário é unicamente responsável pelo ato e nem toda vítima é passiva²⁷⁶. Existe, assim, a possibilidade de se entender que a vítima faz o criminoso em diversos casos e, até, que compõe o rol dos sujeitos ativos²⁷⁷.

Mendelsohn mesmo, ao apontar a vitimologia²⁷⁸, recomenda que:

“O surgimento do papel da vítima em um sistema penal não supõe uma incorporação exclusivamente em benefício da mesma, mas implica compartilhar assim mesmo uma proporção da responsabilidade criminal”.

A partir de tal tendência, é de se entender que delitos são o resultado de vetores da ação do vitimário e da vítima, num comportamento concausal²⁷⁹. Tais vetores podem ter forças em sentidos opostos resultando a) no prevalecimento do vetor da vítima que conseguirá evitar o ato ou b) prevalecendo o vetor do vitimário que conseguirá perpetrar a intenção. Podem, finalmente, os vetores terem mesma direção levando ao cometimento cooperativo do ato e ainda somente existir um único vetor exclusivo da vítima. No primeiro caso, pode-se dizer que o delito é de ação e reação (delitos de intervenção em que há tentativa de impedimento da vítima); no segundo caso, pode-se dizer que o delito é de relacionamento; no último caso, autolesão.

impróprios, g) crimes de atividade ou de resultado, h) crimes de forma livre ou vinculada.

²⁷⁶ VON HENTIG aponta que autor e vítima são verdadeiros sócios na interação criminal. OLIVEIRA, Ana Sofia Schmidt. Op. cit. p. 69.

²⁷⁷ Há uma interessante expressão de Edmundo Oliveira nesse sentido, que é “*La victime éveille l’appétit*” que poderia ser interpretada como “a vítima estimula o apetite” (do vitimário). In Boletim IBCCRIM – Ano 9 - nº 107 – p. 17

²⁷⁸ MENDELSON, Benjamin. “Socio-analytic Introduction to Research in a General Victimological and Criminological perspective”, in *The Victim in International Perspective*, Papers and essays given at the “Third International Symposium on Victimology”, Walter de Gruyter, Berlim, Nova Iorque, 1982, p. 62 *apud* MORENO, Myriam Herrera. “Sobre los Orígenes Científicos de La Victimología”, in *Cuadernos de política criminal*, Editoriales de Derecho Reunidas S.A., nº 56, Madri, Espanha, 1995, p.511.

²⁷⁹ SILVA SANCHEZ, Jesús Maria. “*La consideracion Del comportamiento de La victima em La teoria juridica Del delito*”. Revista Brasileira de Ciências Criminais. Nº 34. Ano 9. Abril-junho de 2001. Editora Revista dos

Acredita-se serem duas as formas através da qual uma vítima se relaciona com o vitimário quando da aproximação delinquente. A primeira seria a aproximação para a vitimização imediata; aqui, não tem o delinquente a intenção maior do que a de conseguir uma curta relação, durante o tempo – ou pelo ato – necessário para que consiga obter perpetrar a conduta almejada: a modalidade, então é de vitimização-fim como nos casos de crimes contra a honra, danos a *sites* alheios ou intrusão informática simples²⁸⁰.

A segunda forma de vitimização é aquela em que os atos de vitimização informática são verdadeiros prelúdios para uma conduta posterior mais grave ou é apenas um ato frente a diversos que se seguirão – repetidos ou não – ensejando, desta feita, violação muito mais grave. A esta forma chamaremos vitimização preparatória ou continuada e tem como ilustrações os delitos de obtenção de números de cartão de crédito através do meio virtual para posteriormente proceder ao uso ilícito dos numerais, a disseminação de códigos maliciosos com o intuito de contaminação, a escravização de máquinas alheias para perpetrar ataques de negação de serviço e até mesmo a violação de *emails* ou programas para obtenção de dados que sirvam de argumentação para extorsão.

Desta forma, existem delitos em que a relação vitimizante produz o resultado ofensivo imediatamente e há relações vitimizantes que são lesões, mas que configuram verdadeiros delitos de meio para o atingimento de um objetivo de implicações mais graves²⁸¹.

Ao tratar-se do parâmetro informático de delinquência, nota-se que a característica da interatividade leva a uma constante troca entre usuarios da rede mundial de computadores, que se comunicam constantemente, criando relações virtuais que podem gerar o delito imediatamente ou preparar delitos subsequentes.

Tribunais. 2001. p. 170.

²⁸⁰ Denominaremos de intrusão informática simples aquela em que o delinquente invade a máquina ou o sistema alheio sem fins que não o de sobrepujar os aplicativos de proteção e defesa do dispositivo e chamaremos de intrusão informática qualificada aquela em que a invasão ocorre com a finalidade de obtenção de dados alheios para os fins de utilização para fins futuros como, por exemplo, extorsão ou falseamento de documentos.

²⁸¹ No caso da vitimização preparatória ou vitimização continuada, é interessante notarmos que de acordo com a proposta de criação dos crimes informáticos a partir da lesão de novos bens jurídicos (confidencialidade, integridade e disponibilidade), os dizeres do instituto da desistência voluntária prevista no artigo 15 do Código Penal parecem-nos inócuos pois que se o agente somente responderia pelos atos praticados, por mais que sua intenção vá mais além do que a da primeira parte da ofensa na vitimização preparatória, ainda assim terá sempre violado ao menos um dos três elementos da segurança informática. Há, pois, que se dizer que ao que nos parece, atos de vitimização preparatória sempre deverão ser punidos.

Por isso e pela essência da rede mundial, toda a navegação pressupõe relações de conexão, inicialmente entre qualquer usuário e um provedor de acesso. A partir dessa interatividade, então, cada usuário decide qual caminho seguirá nas infinitas possibilidades da superautopista, criando outras relações de conexão.

A PRECIPITAÇÃO VITIMAL

Expressão cunhada por Marvin E. Wolfgang, no original “*victim-precipitated*”, serve para descrever as situações em que a vítima contribui amplamente para a ocorrência do delito de forma que sem sua participação o fato não teria ocorrido²⁸². Muito criticada, a expressão recebeu propostas de substituição por nomeclaturas consideradas mais adequadas como “vulnerabilidade da vítima” e “participação da vítima”²⁸³.

Acredita-se que a etiologia vitimal deve ser interpretada sob dois aspectos: um intrínseco e outro extrínseco. O primeiro, a que denominamos perigosidade vitimal²⁸⁴, segue a idéia de que perigo é uma situação que existe independente de fatores interiores do ser humano, ou seja, surge por conta de posturas e interações do indivíduo com o ambiente que o cerca.

O segundo trataria daqueles fatores de predisposição subjetiva em ser vítima de um delito por conta de fraquezas psicológicas – permanentes ou temporárias –, e que servem como facilitadores para a prática de delitos ou facilitadores situacionais e a que chamaremos de receptividade vitimal.

²⁸² MANZANERA, Luiz Rodríguez. Op. cit. p. 146 *apud* OLIVEIRA, Ana Sofia Schmidt de. Op. cit. p.95. Os norte americanos utilizam-se da expressão “*blame the victim*” nesse sentido.

²⁸³ MANZANERA, Luiz Rodríguez. Op. cit. p. 147 *apud* OLIVEIRA, Ana Sofia Schmidt de. Op. cit. p.96.

²⁸⁴ Ainda que a doutrina brasileira tenha acatado o termo “periculosidade” a partir do vocábulo italiano “*pericolo*” para tratar da qualidade de algo ser perigoso, ainda assim a expressão “perigosidade” será adotada pois foi acatada pela doutrina brasileira de tal modo pelo fato de que grandes exponenciais da doutrina vitimológica serem advindos de culturas hispânicas, conforme apresentado ao longo do trabalho desenvolvido.

Perigosidade Vitimal

O termo perigosidade trata da tendência de um indivíduo em ser vítima, seja por causa de uma ação incitativa de um vitimário, seja por conta de atitudes próprias – vitimogenesia criminal²⁸⁵. Assim, é a quantidade de fatores exógenos como locais que frequenta, idade, condição social, altura, peso, falta de companhia, roupas que veste e formas com que se porta que levam alguém a estar mais ou menos suscetível a ser escolhido a ser alvo de uma conduta delinquente ou estar propenso a sofrer danos e prejuízos a partir de suas condutas ou omissões.

A expressão “perigosidade”, em si, traz a ideia de perigo que aqui utilizamos no sentido proposto por Niklas Luhmann de que trata de causa exterior sobre a qual não se tem domínio²⁸⁶.

É curioso apontar que o Brasil tem costume de legislar considerando a perigosidade vitimal. Não bastando o fato de que penas podem ser agravadas, chega-se mesmo a criar normas destinadas à proteção de determinados segmentos, como verdadeiras ações afirmativas que levam ao destaque da vítima como frágil. É o caso do Estatuto do Idoso, Estatuto do Estrangeiro, da Lei Maria da Penha, entre outras legislações.

Porém, os crimes informáticos trazem uma perigosidade vitimal especial, que sofre influência dessa nova parcela social chamada ciberespaço, pois que sua natureza de risco traz periculosidades diferenciadas. O capítulo a seguir será dedicado ao trato da perigosidade frente a algumas categorias de delinquências.

Receptividade Vitimal

Com conceito próximo da ideia de perigosidade vitimal, serve para a construção do raciocínios acerca da previsibilidade de ocorrência de crimes para destinação de políticas criminais focadas, acerca da evitação de suscetibilidade e, também, para o estudo da

²⁸⁵ MORENO, Myriam Herrera. “Sobre los Orígenes Científicos de La Victimología”, in *Cuadernos de política criminal*, Editoriales de Derecho Reunidas S.A., nº 56, Madri, Espanha, 1995, p.512.

²⁸⁶ LUHMANN, Niklas. El concepto de riesgo. In BERIAIN, Josetxo (org.). *Las consecuencias perversas de La modernidad*. Anthropos, Barcelona, 1996, p. 123 e ss. *apud* SOUZA, Luciano Anderson de. *Expansão do Direito Penal e Globalização*. Quartier Latin, São Paulo, 2007, p. 116.

participação destas na gênese do delito. Contudo, a receptividade (ou receptibilidade, ou, ainda, recetibilidade), mais propriamente, é a análise dos elementos de aproximação entre o vitimário e a vítima no que se refere aos fatores endógenos, ou seja, às características pessoais da vítima que a tornam mais propensa para aceitar manipulação, ser persuadida ou assumir estado de fragilidade. Isso se dá pela própria etimologia da expressão, que trata da capacidade ou sensibilidade de algo ou alguém receber fatores ou influências exteriores.

Nas próximas linhas, tratar-se-á da relação entre tais características intrínsecas e pessoais dos usuarios da informática e o impacto destas no sofrimento de um delito, apreciando com especial atenção vítimas sensibilizadas por características como carência, sentimentalismos, curiosidade e até mesmo ganância. Tais fatores terminam por aumentar a potencialidade de alguém, ao se relacionar, ser conduzido ou persuadido.

A PREVENÇÃO VITIMAL

O fato de se compreender que nos delitos de relacionamento as condutas da vítima influem positivamente no exaurimento do tipo traz a reflexão de que a forma como o Direito Penal vinha pensando seus institutos como o do delito, do delinquente e da finalidade da pena possam ser insuficientes para justificarem a delinquência e a violência.

Enquanto os doutrinadores focavam seus estudos na justificativa para a existência do crime no intuito de bani-lo (como se controla uma doença através de vacinação), o resultado foi o de parciais fracassos. Assim, a criminologia presume que o crime é um fenômeno normal da sociedade e que deve ser mantido em patamares mínimos, mas inevitáveis.

Contudo, para atingirem-se tais mínimos, fulcral que se note que a vitimologia traz uma realidade que pode ser interpretada a partir da seguinte metáfora: quando uma criança tem tenra idade, os pais impedem que esta coloque os dedos na tomada retirando-a do local e advertindo-a; assim que a criança cresce, os pais explicam o porquê de terem sempre impedido que esta pusesse a mão da tomada: para evitar choques. Com isso, os parentes evitam desgaste de atenção em ter que, a partir de certa idade de seu filho, manter vigilância acerca desse dever de cuidado entregando, parcialmente e de certo modo, ao filho tal responsabilidade. Resta

então, aos pais, os demais deveres que ainda exigem sua atenção e cuidado. Não houvesse a educação sido dada ao filho e teriam os pais que permanecer numa incessante necessidade de cuidado, dispendiosa e sem futuro porquanto cíclica e infinita.

A vitimologia moderna defende o afastamento da tendência paternalista do Estado e a criação de um Principio vitimológico. Defende que o dispêndio de recursos do Estado deve ser feito respeitando Principios constitucionais como o da eficiência. Destarte, busca-se a genealogia do delito para, uma vez compreendendo-o, evitá-lo a partir de ações de efeitos duradouros.

O esforço dogmático de aperfeiçoamento do estudo do fenômeno delitual, pois, acaba por criar, a partir do desenvolvimento de uma vitimologia mais ampla – denominada “vitimologia do ato”²⁸⁷ –, a ideia de que há a necessidade de se desenvolver um novo pressuposto, uma espécie de competência por parte das vítimas quanto aos delitos e fatos, a partir da ideia de que a nova sociedade pede um novo paradigma de Direito Penal.

A teoria funcionalista (e mais propriamente as teorias de tipo objetivo) leva em conta esse enfoque, compreendendo que a necessidade de aumento das variáveis no conceito de tipicidade leva a um melhor enquadramento das situações, num exercício de justiça. Günther Jakobs, ao focar a teoria, aponta que se deve levar em consideração a existência de uma competência por parte das vítimas a ser analisada²⁸⁸, ou, nas palavras de Myriam Herrera Moreno, uma concepção predispositiva antes somente reservada ao autor do delito²⁸⁹.

Nessa toada, a criação da competência vitimal presume critérios de consciência e educação, que deveriam ser uniformizados e difundidos para uma possível prevenção, além de responsabilidade no que se refere a seus bens jurídicos disponíveis, administrados sob alçada particular – a irresponsabilidade sobre os próprios bens jurídicos geraria verdadeira autocolocação em risco e violaria a ideia de merecimento de proteção penal.

A maior liberdade e complexidade de pensamento trazido pelas teorias pós-finalistas

²⁸⁷ MORENO, Myriam Herrera. “Sobre los Orígenes Científicos de La Victimología”, in *Cuadernos de política criminal*, Editoriales de Derecho Reunidas S.A., nº 56, Madrid, Espanha, 1995, pp.511-512.

²⁸⁸ JAKOBS, Günther. *A Imputação Objetiva no Direito Penal* (tradução André Luis Callegari), 2ª Edição. Editora Revista dos Tribunais, São Paulo, 2007, Pp. 78-79.

²⁸⁹ MORENO, Myriam Herrera. Op. cit., p.512.

levaram a questionamentos sobre a teoria da pena e suas finalidades, tendo-se em vista que a ação focada somente na figura do delinquente mostraram ter efeito de contenção parcial²⁹⁰.

O Estado que pune criminosos pelo simples fato de buscar a prevenção geral e individual não atinge completamente seus objetivos. Isso porque por conta da perigosidade vitimal ser um fator relevante, deve-se voltar atenção à vítima como apoio e reforço na questão delinquente. A partir de tais ideias, comprovadas por adágios da sabedoria popular como o de que “errar é humano mas insistir no erro é tolice”, e de que “não adianta dar o peixe, deve-se ensinar a pescar”, a vitimologia percebe que o foco restringido ao delinquente faz com que a ação penal seja verdadeiro descarte de recursos para mero cumprimento do dever do Estado em reagir ao fato violador de bens jurídicos.

Hassemer aponta claramente a importância da evitação criminal e do aumento de responsabilidades dos particulares quanto aos riscos que o cercam, expondo que:

“Um Direito Penal orientado pela prevenção vê a vítima sob o ponto de vista da profilaxia; e se limita a advertir especialmente as vítimas de lesões (idosos, crianças e os pais, proprietários, agências bancárias, políticos) e a protegê-las em caso de necessidade. O Princípio da retribuição e da satisfação é substituído pelo Princípio da segurança e da assistência”²⁹¹

É de se lembrar que a já citada Resolução 40/34 da Assembleia Geral das Nações Unidas aponta a importância da prevenção, especialmente em seu item 5, letras “b” e “c” ao propugnar ser mote das nações

“b- patrocinar as investigações práticas de caráter cooperativo sobre os meios de reduzir o número de vítimas e prestar auxílio às vítimas, e promover intercâmbios de informações sobre os meios

²⁹⁰ Também interessante notar que Eugênio Raul Zaffaroni, no 14º. Congresso Internacional de Direito Penal promovido pelo IBCCrim em 2008, em que defende que a criminologia “morreu” no momento em que surgiram crimes contra a humanidade e atos terroristas, que se mostraram inexplicáveis às vistas das teorias do autor clássicas, exigindo, para isso, teorias de anulação de responsabilidade, demonstrando a superação do foco exclusivo.

²⁹¹ HASSEMER, Winfried. Introdução aos Fundamentos do Direito Penal. Sergio Antonio Fabris Editor. Porto Alegre. 2005. pp. 116-117

eficazes de alcançar esses fins; e

c- prestar ajuda direta aos governos que a solicitem com intuito de auxiliá-los a reduzir o número de vítimas”.

Especialmente acerca da criminalidade informática, a Organização das Nações Unidas elaborou um “Manual sobre prevenção e controle de crimes relacionados com computadores” em que é feita uma análise dos principais problemas quanto a tal vitimização e que é abordada a proposta de política criminal ao final do trabalho.

ABORDAGEM VITIMODOGMÁTICA DOS DELITOS INFORMÁTICOS PRÓPRIOS PUROS

Uma vez que surja o conformismo que os delitos informáticos podem ser tidos ou como uma nova forma de se praticar velhos delitos – uma nova ferramenta – (delitos informáticos impróprios) ou como ações novas que violam bens jurídicos antigos (delitos informáticos próprios impuros) e/ou valores e bens jurídicos novos (delitos informáticos próprios puros), é fundamental que se aceite que, no meio informático, certas características particulares das vítimas influenciam em sua potencialidade vitimal e na própria criminogênese.

Isso se dá por conta de situações particulares que, cruzadas com a realidade criada pela informática, geram consequências relevantes para o estudo da vitimização. Assim,

“Nossa confiança, apetite e necessidade por tecnologia, embora nos traga prazer e informação e seja bastante necessária, também se está transformando rapidamente numa fonte de vitimização. Como sempre, há quem tenha a inclinação e o conhecimento para explorar os benefícios da tecnologia para fazer com que os vulneráveis, os jovens, os imaturos, os inocentes e os gananciosos se tornem vítimas”²⁹²

O Código Penal já cria em seu artigo 61 uma lista de vítimas consideradas especialmente distintas e que sua ofensa leva a um agravamento da pena, quais sejam a vítima familiar (inciso “e”: ascendente, descendente, irmão ou cônjuge), a vítima sob autoridade ou em situação de relação doméstica (inciso “f”: abuso de autoridade ou prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade ou com violência contra a mulher), a vítima em situação de relação laboral ou hierárquica (inciso “g”: abuso de poder ou violação de dever inerente a cargo, ofício, ministério ou profissão) e a vítima em condição peculiar (inciso “h”: criança, maior de sessenta anos, enfermo ou mulher grávida; e inciso “i”: ofendido em situação de desgraça particular).

²⁹² ALBUQUERQUE, op. cit. Prefácio, p. XV.

Note-se que apesar de a “*labelling approach*” ser formulada como uma teoria criminológica, para muitos de rotulação de autores, em verdade ela é representada por uma reação crítica “*ao sistema de controle social e suas consequências, bem como ao papel exercido pela vítima na relação delitual*”²⁹³. Por isso, cremos possa ser aplicada no que se refere à vítima pois que há verdadeiro processo de seleção e estigmatização das vítimas²⁹⁴.

Certamente que a reação crítica de tal movimento fez com que a ideia de inter-relação entre indivíduos fosse trazida à baila, crescendo-se o conceito de que o ser humano varia sua personalidade nas diferentes fases da vida, nos diferentes grupos que frequenta e com diferentes pessoas com as quais se relaciona.

Assim, acaba a teoria por defender que, por conta das relações os seres humanos costumam se estigmatizar (simplificando a crítica a um conceito fechado) e, por isso, uma delinquência secundária irá surgir a partir de conceitos comparativos e antagônicos de comportamentos sociais: de um lado há o aceitável e por outro, o desviante (*deviance*).

Para nós, essas ideias são aplicáveis à vitimologia: também há condutas aceitáveis por parte de vítimas, há condutas desviantes, e até mesmo é possível rotular-se espécies de pessoas que são alvo de política legislativa especial por seu pressuposto estado especial, além do fato de que a sociedade costuma rotular vitimizadas como fracas. A forma como Alessandro Baratta define, pois, a teoria do *labelling approach* e que aqui aprouve é a de que é

*“a investigação criminológica tem tendência para se deslocar das causas de comportamento criminal em direção às condições a partir das quais, numa dada sociedade, as etiquetas da criminalidade e o estatuto do criminoso são atribuídos a comportamento e a sujeitos, e para o funcionamento da reação social informal e institucional”*²⁹⁵

Por isso, afora o fato de o Código Penal verdadeiramente etiquetar (e a sociedade

²⁹³ SHECAIRA, Sergio Salomão. Criminologia. Ed. RT. 2008. São Paulo, p. 269.

²⁹⁴ CÂMARA, Guilherme Costa. Op. cit. pp. 83-86.

²⁹⁵ BARATTA, Alessandro. Sobre a criminologia crítica e sua função na política criminal. Separata de Documentação e Direito Comparado (Boletim do Ministério da Justiça), n. 13, p. 147 *apud* SHECAIRA, Sergio Salomão. Criminologia. Ed. RT. 2008. São Paulo, p. 320.

também) a vítima, presumindo fraquezas e presumindo situações, acredita-se que na criminalidade informática se lida com novas situações, algumas criadas, outras potencializadas pela tecnologia.

Decidimos, assim, por analisar alguns perfis de sujeitos (ou de situações em que sujeitos podem se encontrar) que são consideradas relevantes para a análise da perspectiva vitimológica da dogmática penal. Destaque para o fato de que algumas vítimas (ou situações geradoras de receptividade vitimal) chegam a ser especificações da ideia de vítima provocadora de Fattah²⁹⁶. Isso porque nessa concepção há vítimas que incitam o delinquente a cometer a infração de dois modos: ativo e passivo, respectivamente através da provocação direta e indireta.

A provocação indireta é causada por ações negligentes ou imprudentes e propiciam e favorecem a prática delitual, incitando o delinquente. Nesta figura se situa a figura da “*contributory negligence*” do direito anglo-saxão em que se aceita verdadeiramente a possibilidade de vítimas (reais ou virtuais²⁹⁷) terem responsabilidades de cautela.

Já a provocação direta é verdadeiro dolo para causação de uma ação delinquente contra si ou outrem.

Embasados nos principais delitos informáticos próprios puros e nas características da informática e do meio computacional, optou-se por um rol de vítimas que trazem forte impacto na gênese delinquente. São elas a vítima solitária, a vítima ignorante, a vítima idosa, a vítima criança ou adolescente, a vítima gananciosa e a vítima curiosa.

A VÍTIMA SOLITÁRIA

Não há dúvida de que a informática, em seu braço mais próximo do usuário, prima pela individualidade. Desta forma, a interface através da qual o cidadão interage com as tecnologias da informação foi desenvolvida para ser utilizada somente por uma pessoa por

²⁹⁶ *Apud* NEUMAN, Elias. *Victimologia*. Editorial Universidad. Buenos Aires. 1994. pp. 53-54

²⁹⁷ Também denominadas “vítimas potenciais”, são aquelas que “comparecem moduladas por notas de incerteza do que está por vir”. CÂMARA, Guilherme Costa. *Op. cit.* pp.111-119.

vez, certamente também para poupar violações de privacidade. Veja-se o exemplo de caixas eletrônicos, aparelhos celulares, *notebooks* e até mesmo tocadores de música – todos focados para o uso simples.

O fato de muitos serviços utilizados por diversos tipos de profissionais estarem integralmente dependentes da tecnologia, e pela quantidade de informação disponível ser muito sedutora, torna-se cada dia maior o espaço de tempo em que as pessoas permanecem conectadas ou em contato com dispositivos de informática, de regra sozinhas.

Com isso, é possível dizer que se por um lado a tecnologia tem duas vertentes: de um lado aproxima as pessoas por permitir maior velocidade e intensidade nos contatos, através de *emails*, mensagens SMS e MMS, redes sociais, entre tantos; por outro lado, restringe e cerceia o contato físico entre humanos, restringe trocas e diminui a sociabilidade, que tem perdido espaço gradualmente.

O termo solitário utilizado nesta tentativa de classificação vitimal somente tem cabimento quando se reflete ao crime informático. Isso porque há uma intensa exposição a riscos na rede mundial de computadores, tanto na modalidade ativa quanto passiva.

Exposição informática passiva a riscos é a conduta de navegação simples e uso seguro de tecnologias. A exposição ativa, por sua vez, pode ser compreendida como a navegação e uso em que não há a preocupação com segurança, chegando à imprudência e até a colaboração ao processo de vitimização. No primeiro caso, tem-se a navegação em *sites* seguros e confiáveis, além do uso de aplicativos de segurança, mas que ainda assim admite a ação de um vitimário que busca por usuarios propensos, e que, em seguida, promove ataque lesionador de bens jurídicos por condutas exclusivamente suas. Exposição ativa, ao revés, é a atitude vitimal facilitadora e contribuinte para a vitimização como nos casos de acesso a páginas inseguras, ou de conteúdo duvidoso.

Duas são as formas de solidão que devem ser consideradas para este trabalho: a solidão antisocial e a solidão relacional. A primeira seria a falta de convívio real no meio social, temporária ou duradoura, que se denomina solidão propriamente dita. A segunda, por sua vez seria a solidão por conta de uma carência afetiva, ou a falta de uma companhia que geraria, assim – instintivamente até –, a procura por uma parceria para completar-se, seja para uma

amizade, seja para um relacionamento.

Uma pessoa pode estar isolada mas gostar do convívio social, fato que procurará realizar futuramente, ou pode estar isolada e não se interessar pelo entrosamento com outros. Uma pessoa sociável pode não ter relacionamentos afetivos, assim como uma pessoa não sociável também pode não tê-los. E, finalmente, tanto pessoas sociáveis quanto não podem ter relacionamentos afetivos que as satisfaçam.

O que se pretende apresentar, nesta etapa, é a suscetibilidade dos perfis solitários a serem vítimas de crimes informáticos. Para isso, desenvolveu-se o estudo a partir de um²⁹⁸ *paper* desenvolvido por Shim e Lee, apresentado na Associação de Comunicação Internacional, em Dresden, Alemanha, em que, a partir de estudos comportamentais, concluiu-se que há predisposições vitimais para a exposição de pornografia não solicitada, atrativo de alta suscetibilidade.

A Solidão Antissocial

Boa parte da criminalidade informática está artilhosamente maquiada por mecanismos de engenhosidade social na criação de golpes. Invariavelmente, grande é a proporção de golpes que utilizam o subterfúgio da pornografia ou da relação íntima para se instalarem.

A partir dos estudos da tendência da sexualidade e a tendência à antisociabilidade (descoberta a partir do teste de Eysenck²⁹⁹), concluiu-se que há diferentes tendências para usuarios aproximarem-se de materiais pornográficos, que podem eventualmente ser arapucas que escondem métodos de violação de direitos.

Uma conclusão interessante do estudo é a de que pessoas com mais tendências antissociais são muito mais tendentes a consumir materiais de sexo explícito. O estudo faz referência a uma pesquisa canadense promovida por Bogaert, em 2001, em que este aponta,

²⁹⁸ SHIM, J. and LEE, S. "Who Wants to Respond to Unwanted Sexually Explicit Materials on the Internet? From an Individual Difference Perspective" *Paper presented at the annual meeting of the International Communication Association, Dresden International Congress Centre, Dresden, Germany Online* <APPLICATION/PDF>. http://www.allacademic.com/meta/p92926_index.html. Acesso em 05.10.08 às 15:25hs.

²⁹⁹ Hans Jurgen Eysenck foi um psicólogo alemão que, dentre outros estudos, desenvolveu um método avaliativo da personalidade humana através de um teste capaz de quantificar três itens: a) a sociabilidade humana - extroversão, b) a capacidade de sentir emoções - neuroticismo, e c) o potencial de rebelar-se (sentido

com maior detalhamento, que pessoas antissociais têm tendência a consumir cinco tipos de materiais pornográficos pela rede: eróticos, insaciáveis, violentos, infantis e pornografia com história³⁰⁰.

Todavia, a mera característica de alguém ser antissocial não bastará para tais condutas. É de se apresentar, também, a ideia das figuras da erotofilia e da erotofobia – medidas de acordo com a forma como alguém reage quando estimulado sexualmente – , pois influem diretamente, também, na conduta *online* de um usuário.

Diversas características foram apontadas para a predisposição do usuário. A primeira refere-se à afinidade que alguém possui quanto ao conteúdo sexual liberal e a segunda, ao conservadorismo. Outra delas é o fato de que usuários erotóforos são mais interessados em conteúdos de sexualidade tradicional e são menos influenciados a aceitar o estímulo sexual promovido por um *site* com um *link* com dizeres “clique aqui” que promete conteúdo pornográfico atípico. Em contrapartida, erotófilos são mais propensos a aceitar estímulos e armadilhas virtuais que prometam conteúdo sexual de toda a natureza bem como produtos contraceptivos e informações sobre sexualidade. Há, pois, maior reação positiva quando a provocação virtual atinge erotófilos.

Com isso, a forma com que se deve interpretar as conclusões é no sentido de que usuários com perfis antissociais³⁰¹ são mais propensos a acessar pornografias a ele ofertada do que usuários sociais, sendo tal um fator influenciador. Também, é conclusivo que indivíduos erotófilos sejam melhores alvos para promessas de material com conteúdo pornográfico pois que não sofrem as mesmas limitações de gosto que usuários erotóforos (que conhecendo o quão explícitos podem ser certos materiais *online*, evitam contato). Assim, *a fortiori*, conclui-se que estarão, também, mais propensos a cair em armadilhas e golpes que envolvam tais materiais, aqueles indivíduos que têm menos contato social (e portanto são mais sós) e que cumulativamente são mais liberais na concepção de gostos sexuais.

De tal modo, a exposição ativa a riscos na rede mundial de computadores é menor aos usuários mais sociais (menos antissociais) pois possuem menor tendência (até impulsiva) a

comportamental) - psicoticismo. <http://www.indiana.edu/~intell/eysenck.shtml>. Acesso em 04.10.08 às 19:21hs

³⁰⁰ Com isso, concluiu que tais usuários apresentam quatro características relativas a seus consumos: agressão sexual, hipermasculinidade, maquiavelismo e psicoticismo.

³⁰¹ O estudo chama de “*psychopaths*” ou portadores de “*psycopath personality*” (psicopatas ou portadores de

aceitarem as corriqueiras propostas virtuais de acesso a material de conteúdo sexual. Em contrapartida, usuarios mais antissociais apresentam tendência a buscarem na rede satisfações, no intuito de reverter frustrações pessoais e, assim, mostram-se mais propensos a aceitação de convites a materiais pornográficos que comumente escondem códigos maliciosos que abrirão *backdoors* na máquina do usuario, contaminarão com programas de replicagem automática para violação de disponibilidade ou até mesmo para espalharem mensagens comerciais e até mesmo infiltrarão programas aparentemente inofensivos mas que terminam por obter senhas e numerais importantes para o usuario. Diante disso, é de se concluir que a solidão física prolongada seria capaz de influenciar negativamente a criminalidade, aumentando o potencial de vitimização de usuarios.

Some-se a isso o segundo fator, acerca da preferência por conteúdos relacionados com a sexualidade humana que também serve de variável de consideração obrigatória. Usuarios denominados erotófilos, por terem interesse no consumo de materiais pornográficos não tradicionais, veem na rede (por sua liberdade de informação, anonimato e sensação de segurança, principalmente) uma biblioteca infindável de conteúdo alternativo (por alguns chamados de desviantes) como sexo com violência, zoofilia, coprofilia, *bondage*, etc.

Tendo-se em vista o interesse (ou curiosidade) sexual em áreas pouco comuns, tal usuario simpatiza mais com o ambiente virtual que lhe concede tais produtos, ficando mais propenso à aceitação a convites para acesso a conteúdos de tal natureza, vez que conhecem tal característica da rede. Em contrapartida, usuarios erotófobos, considerados aqueles que preferem linhagem tradicional ortodoxa de sexualidade, pelo mesmo motivo de saberem os tipos de conteúdo que a rede oferece, e por não terem seu gosto (interesse) voltado a tais práticas, é menos propenso a convites de natureza sexual pelo ciberespaço.

Por isso, usuarios antissociais (com aversão a socialização ou, ainda, dificuldade de socialização) apresentam maior receptividade vitimal para crimes informáticos que se utilizam da máscara da pornografia, que pode ser ainda mais potencializada pelo gosto por sexualidade desviante (erotofilia)³⁰².

personalidade psicopata).

³⁰² Tomamos o cuidado de evitar a discussão acerca da vítima sexualmente compulsiva, tendo-se em vista que o desvio de personalidade afasta dela a capacidade de balancear os riscos do acesso a sites arriscados ou perigosos.

A Solidão Relacional

Como já apontado, o termo solidão relacional está diretamente ligado com a ideia de carência afetiva, de falta de companhia. Neste aspecto, não há o raciocínio da antissociabilidade, mas sim a ideia de vontade de sociabilizar e que utiliza do meio informático para isso.

Conforme já houve oportunidade de dizer, a rede mundial tem grande potencial comunicativo. Há, todavia, grande diferenciação entre a comunicação e a socialização. Aliás, por tal motivo que é possível falar de usuarios de Internet antissociais: porque mesmo estando em constante comunicação e troca de informações, ainda assim não são (ou são pouco) capazes de lidar na sociedade real.

Contudo, há pessoas de índole sociável mas que passam por períodos de falta de companhia e isso acaba por gerar sensação de solidão. Certamente que o ser humano precisa de pessoas por ser social por natureza, como disse Marx. Ainda que se considere que a solidão física meramente como um estado de falta de outrem, é sabido que a solidão afetiva não pode ser com esta confundida.

A necessidade do ser humano em se relacionar com amigos, parentes e companhias do sexo oposto ou do mesmo sexo é tão importante para a saúde mental quanto a alimentação. Por isso, é instintiva ao homem a busca por relacionamentos até mesmo para que possa encontrar tranquilidade e até mesmo a procriação. A permanente falta de companhias, pois chega até mesmo a gerar implicações psicológicas pois que o “*homo sociabilis*” necessita compartilhar³⁰³.

Assim, a busca por pessoas com afinidades, grupos semelhantes e relacionamentos afetivos ou sexuais é natural no ser humano. O advento da informática aumentou a capacidade de publicidade de empresas e igualmente a capacidade de *marketing* pessoal dos usuarios que em boa quantidade mostram-se ávidos por usar a ferramenta com cunho social.

Os principais usos da rede estão diretamente voltados para relacionamentos ou meios

³⁰³ DIMARCO, Heather. The electronic cloak: secret sexual deviance in cybersociety. In Dot.Cons. Willan Publising, Devon, 2003, p. 53.

intermediários para tais. A criação do *email*, dos comunicadores instantâneos e até mesmo das redes sociais como por exemplo o *Orkut*, o *MySpace* e o *Facebook* são exemplos explícitos do sucesso que são as ferramentas para a comunicação e relacionamento. Contudo, há ainda serviços específicos que exploram a vulnerabilidade humana causada pela solidão. Busca por acompanhantes, serviços de auxílio para encontrar noivas, apoio para adoção internacional de bebês, intermediação para prostituição, salas de bate-papo de encontros, são apenas alguns exemplos de serviços disponíveis em abundância na rede³⁰⁴. E por serem serviços que exploram o momento humano em que há a fragilidade advinda da falta de companhia, com certa frequência são utilizados para conseguir a confiança dos usuarios, diminuir-lhe a resistência, e então promover alguma atitude prejudicial a seus bens jurídicos.

Não raro relacionamentos virtuais duradouros são construídos com o único intuito de conseguir informações privilegiadas da vítima. Não raro *sites* são construídos para dar impressão ao usuario de que oferece serviços, quando em verdade está-se ludibriando o solitário retirando-lhe dinheiro e entregando-lhe falsa esperança. Não raro o *site* é espelho para programas maliciosos serem instalados no computador alheio, obtendo número de cartão de crédito ou outras informações sensíveis.

Indubitavelmente, o usuario interessado em novas companhias, costuma confiar em serviços de auxílio e apoio a tais fins, tendo, por conta da emoção advinda do estado de solitude, certas capacidades cognitivas diminuídas em detrimento de sua necessidade. Desta maneira, o vitimário, conhecendo essas particularidades, explora tal estado emocional, aproveitando-se da mitigação da defesa no ambiente de risco³⁰⁵.

A VÍTIMA IGNORANTE

A ignorância é tratada de diversos modos pelo direito. De um lado, o artigo 3º da Lei de Introdução ao Código Civil aponta que ninguém pode alegar desconhecimento da lei para

³⁰⁴ LETHERBY, Gayle e MARCHBANK, Jen. Cyber-chattels: buying brides and babies on the Net. In Dot.Cons. Willan Publishing, Devon, 2003, pp. 68-85.

³⁰⁵ Aqui cabe a reflexão acerca das situações constantes no artigo 61, II, incisos “c” e “j”; o primeiro inciso trata do crime cometido em circunstância que dificulte ou impossibilite a defesa da vítima e o segundo, o “estado de desgraça particular do ofendido”. Ambos servem de agravante para majorar a pena do vitimário, contudo, é de se

escusar-se, quanto à sua conduta. Em seguida, o Código Penal em seu artigo 21 apresenta que o desconhecimento da lei é inescusável, dando ao erro o condão de isentar o agente de pena, somente em casos escusáveis.

Ao tratar-se da vítima ignorante, não se está almejando uma reflexão sobre seu desconhecimento legal, todavia. A discussão vitimológica, nesta etapa, se dá pela compreensão global do usuário informático quanto ao meio em que vive, o que imediatamente pressupõe algum conhecimento em informática e também a capacidade de visualizar o novo ambiente de interação humana.

Para a justa aplicação da pena e para a correta aplicação das circunstâncias judiciais do artigo 59 do *códex*, imprescindível é que se veja se e o quão imprudente foi a vítima³⁰⁶ e o quão possível era o grau de precaução que deveria ter sido tomado, no raciocínio de um Princípio de autoresponsabilidade.

A ignorância referida tem dois aspectos: a ignorância dos riscos da rede e a ignorância informática. Ambas as formas de ignorâncias devem ser apreciadas casuisticamente, *ex post*, tendo-se em vista a necessidade de quantificação de sua participação no fato.

A primeira modalidade acredita-se que evolui para um fim. Ainda que boa parte dos cidadãos não seja detentor de acesso à Internet³⁰⁷, o ingresso no meio é cada dia que passa mais notoriamente a entrada para um universo de criminalidade em que se está permanentemente frente a relações potencialmente vitimizadoras. Portanto, ignorância quanto à periculosidade da rede mundial de computadores em sentido amplo é argumento de crescente duvidosa aceitabilidade em tempos modernos, tendo-se em vista a larga inserção educativa da mídia (e até mesmo dos pais e professores) nesse sentido.

É de se dizer que assim como há uma maioria penal que representa a culpabilidade do ofensor pelo critério biopsicológico – num misto de amadurecimento biológico e

questionar qual seria o instituto mais adequado no caso concreto.

³⁰⁶ NUCCI, Guilherme de Souza. Individualização da Pena, 2ª edição revista, ampliada e atualizada. Editora Revista dos Tribunais, São Paulo, 2007, p. 208.

³⁰⁷ De acordo com a empresa Jupiter Research, cerca de um quarto do mundo estará na Internet até 2012, totalizando cerca de 1,8 bilhão de usuários conectados. Disponível em http://www.jupiterresearch.com/bin/item.pl/press:press_release/2008/id=08.06.23-economies-will-power%20.html/. Acesso em 04.10.08 às 02:18hs.

capacidade de compreensão –, analogamente se pode raciocinar um verdadeiro amadurecimento da vida virtual.

O novo usuario (*newbie* ou ciberturista), inicialmente engatinha no meio virtual, vendo com ilusões a navegação, a quantidade de informações e mesmo o potencial multimídia. Aventura-se pelos meandros informáticos, pelos serviços como *emails*, comunicadores instantâneos, blogs e microblogs (como o *Twitter*), navega por *sites* desde oficiais até de natureza duvidosa, baixa arquivos e assim por diante. E é por inicialmente não depender em demasia da tecnologia e porque há certo empirismo no conhecimento informático, que termina o usuario por sofrer seus primeiros ataques, ser contaminado pelo primeiro código malicioso e sofrer os primeiros prejuízos. A tendência, então, é a evolução natural a partir dos dissabores, resultando num portar-se mais cauteloso pelo aprendizado com erros virtuais do passado.

Mas a rede não evolui e amadurece individualmente. Os primeiros usuarios consuetudinariamente passam a seus alunos e descendentes as experiências prejudiciais do uso da informática e estes absorvem. A rede como um todo amadurece e certos riscos passam a ser eliminados pela prevenção e pela educação, eliminados por perderem sua razão de existir ou, ainda, mantém-se ativos, mas com reduzido índice de eficiência. O aprendizado do cibercomportamento delinquente, quando arraigado, leva a uma tolerância dos usuarios do meio, que consideram tal risco como aceitável e as vitimizações a partir de tais atos deixam de ser escusáveis.

Certamente, a engenhosidade social cria novas situações e novos ardis para o cometimento de crimes informáticos; porém, mais e mais os golpes são divulgados e, em alguns níveis sociais e de educação, a alegação de ignorância da vítima perde a credibilidade do mesmo modo que golpes como o do bilhete premiado são de inaceitável vitimização frente a uma pessoa culta.

A parcela de culpa por parte da vítima ignorante, assim, depende do grau de inevitabilidade existente quanto à prática e a possibilidade de o usuario, se diligente e prudente, ter evitado a ação. Aqui se trata dos crimes de relacionamento em que o uso de engenhosidade é o único meio através do qual a figura se perpetra. A dificuldade de tais ações reside na dinâmica da informática, dos serviços prestados e principalmente dos usuarios mal

intencionados que se mostram capazes de criar sempre novas formas de perpetrar golpes e persuadir usuarios com boa técnica, fazendo as perguntas certas e passando alguma credibilidade.

Outra hipótese de ignorância – esta de maior complexidade – é a figura da ignorância tecnológica. Como apenas uma mínima parte dos usuarios possui sólidos conhecimentos técnicos na área de informática, tais noções mostram-se pedras de toque para indivíduos mal intencionados e que tem como intuito gerar vantagens próprias. A linguagem própria da rede mundial de computadores, a forma como os programas são escritos, as tecnologias de informação utilizadas e até mesmo conhecimento em funcionamento de redes serve como instrumento especial nas mãos de quem sabe manejá-lo. A partir de tal cultura, um usuario pode facilmente subjugar outro e tomar controle de sua máquina, violando direitos em detrimento da segurança informática.

Um usuario comum sendo atacado na rede mundial de computadores por um experto em informática sofrerá um ataque tão desproporcional e iníquo quanto uma avalanche sobre casas de sapé. Por isso, as ferramentas de proteção são criadas para automaticamente criarem barreiras de proteção a ataques e tentativas de invasão.

Exemplificativamente, um estudo promovido pelo grupo *SiteAdvisor* criado por engenheiros do MIT – *Massachusetts Institute of Technology* – concluiu que 97% dos usuarios são incapazes de identificar um *site* legítimo de um *site* armadilha para difusão de códigos maliciosos³⁰⁸.

Ocorre que o potencial explorador de *hackers* e *crackers* e a habilidade em descobrir falhas de segurança e *bugs* é significativamente superior à capacidade de resposta por parte de programadores de segurança digital. Não raro demoram-se meses para descobrir uma brecha que vem sendo explorada para alguma conduta lesionadora.

E aí está o principal problema da ignorância informática. Por conta de uma cultura de automatização de processos e encobrimento de acontecimentos, os usuarios acomodam-se na ignorância informática, terminando por tornarem-se vítimas que sequer notam os fatos

³⁰⁸ Em http://idgnow.uol.com.br/seguranca/2006/04/27/idgnoticia.2006-04-27.1666584131/IDGNoticia_view/.

sofridos.

Curioso notar que pesquisa do *site* “*ThisIsMoney*” revelou que boa parte dos usuários de Internet da Grã-Bretanha são negligentes e relaxados quanto a procedimentos de segurança *online*, chegando-se a ponto de metade dos usuários que sofreram ataques virtuais em que dinheiro foi retirado de suas contas correntes sequer sabiam do acontecido. A mesma pesquisa revelou que o número de pessoas tendentes a usar *sites* não confiáveis para fazerem compras permanece alto e dois terços dos usuários de uma bandeira de cartão de crédito acreditam que a fraude *online* é uma ameaça longínqua³⁰⁹.

Quanto à informática, porém, tribunais brasileiros já se manifestaram no sentido de que apesar da ignorância de boa parte do povo brasileiro quanto aos métodos utilizados pelos delinquentes informáticos, ainda assim, nos casos de clonagem de cartões de crédito, por exemplo, cabe à vítima a prova de que o banco agiu com negligência, imperícia ou imprudência na entrega do dinheiro ao agente, cabendo ao banco o ônus de provar ter havido culpa exclusiva ou concorrente da vítima³¹⁰.

A VÍTIMA IDOSA

Protegido pela lei 10.741/2003, também denominada estatuto do idoso, o cidadão com idade acima de sessenta anos possui tratamento diferenciado em diversas esferas, além de conservar, evidentemente, todos os direitos relativos a qualquer pessoa humana (desnecessariamente reafirmado pelo artigo 2º da aludida lei).

O Direito Penal criou tipos penais específicos para a proteção de tal categoria de indivíduos, sempre voltados para coibir a discriminação da pessoa de idade, o impedimento a acessos, e até uma omissão de assistência (art. 97 da Lei 10.741/03), o abandono de incapaz

Acesso em 03.10.08 às 03:14hs.

³⁰⁹Em http://www.thisismoney.co.uk/news/article.html?in_article_id=405615&in_page_id=2. Acesso em 03.10.08 às 03:36hs.

³¹⁰ Posições do TRF da 1ª região e do Superior Tribunal de Justiça, conforme <http://revistaepoca.globo.com/Revista/Epoca/0,,EDG67166-6012,00-CORRENTISTA+DEVE+PROVAR+CULPA+DO+BANCO+EM+SAQUES+IRREGULARES.html>. Acesso em 03.10.08 às 03:41hs.

especial (art. 98), a exposição ou maus tratos especial (art. 99), etc.

Indiretamente quanto ao temário (não é um crime informático, mas sim um crime que envolve a informática), houve a criação de uma conduta no artigo 104 do estatuto, punindo com detenção de 6 (seis) meses a 2 (dois) anos aqueles que retêm o cartão magnético da conta bancária relativa a benefícios, proventos ou pensão do idoso, com objetivos de ressarcimento ou recebimento de dívidas³¹¹.

Dentre os crimes virtuais, é de se dizer que há uma necessidade especial de se avaliar tais condutas, levando-se em conta a natural fragilidade dessa classe de indivíduos. Reforço quanto ao argumento de especial importância está no artigo 61, II, “h” do Código Penal, que foi alterado pela Lei 10.741, acrescentando-se a pessoa de idade vítima como circunstância agravante da pena.

O avanço da idade traz uma diversidade de alterações somáticas que podem influenciar o estado psíquico humano. No que tange à criminalidade informática e as tecnologias envolvidas, são características a serem consideradas a natural perda de visão acurada e as alterações de sono, ambas capazes de influenciar no cometimento de fatos delinquentes tendo-se em vista que (i) por vezes são indícios de início de delinquência pequenas e sutis alterações na tela de programas, e (ii) boa parte dos crimes de relacionamento de dá em salas de bate papo. Conhecendo-se a rotina insone das pessoas de idade, aquelas que passam o tempo acordadas em tais passatempos, certamente freqüentam um ambiente de batante interesse por parte dos vitimários.

Além disso, o envelhecimento traz consigo outras características que influenciam diretamente a vitimização: são algumas delas a dificuldade acentuada em adaptar-se a novas tecnologias e sua linguagem, a não compreensão de certos serviços ofertados pela informática e, principalmente, a não compreensão dos valores dos bens jurídicos virtuais, o desconhecimento de limites das atitudes dos delinquentes, e o potencial prejudicial da ação delituosa.

³¹¹ Art. 104. Reter o cartão magnético de conta bancária relativa a benefícios, proventos ou pensão do idoso, bem como qualquer outro documento com objetivo de assegurar recebimento ou ressarcimento de dívida: Pena – detenção de 6 (seis) meses a 2 (dois) anos e multa.

Tais desconhecimentos geram uma fragilidade especial no que toca a imprudência de navegação – como a abertura de anexos duvidosos de pessoas conhecidas ou navegação por *sites* armadilha que prometem companhia para terceira idade ou remédios a preço baixo –, imprudência na instalação de programas – como na dificuldade de diferenciar programas íntegros de programas duvidosos – na atualização de programas de segurança – que exigem cuidados diários – e mesmo na crença exagerada em notícias ou identidades de mensagens de *scamming*.

A VÍTIMA CRIANÇA/ ADOLESCENTE

Inicialmente, é importante que se coloque uma crítica ao modo como a doutrina e a legislação costumam tratar, como se fossem uma só categoria, a criança e o adolescente³¹². Exemplo disso são os delitos do Estatuto da Criança e do Adolescente, que tratam do mesmo modo e com os mesmos limites de pena crimes em face de ambas vítimas, sem levar em conta o grau de desenvolvimento intelectual ou sexual, o que proporciona uma desproporcionalidade tanto na aplicação da pena quanto do critério legislativo de apresentação dos *quantum* mínimo e máximo.

Os diferentes estágios da vida certamente exigem cuidados diferenciados quanto à educação e restrição de exposição aos riscos. De tal monta, ao entrar para a adolescência, um indivíduo já busca maior independência e autonomia quanto às tarefas do dia a dia, ficando, assim, mais sujeito a influências externas. Certamente, também, no estágio da adolescência as alterações metabólicas levam ao afloramento da sexualidade e à curiosidade quanto às práticas neste sentido.

O que se quer, desta forma, é chamar a atenção para o fato de que crianças e

³¹² Há um recente exemplo interessante nesse sentido, qual seja a Convenção de Proteção da Criança contra a Exploração Sexual e Abuso Sexual - Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.: 201) – de 25 de outubro de 2007, em que consta, em seu artigo 3º que trata das definições do normativo, os seguintes dizeres “criança, deverá significar qualquer pessoa com idade inferior a 18 anos (“child” shall mean any person under the age of 18 years), o que reforça a ideia de que o tratamento, em boa parte dos casos, ignora a questão das diferenças psicológicas e de desenvolvimento de tais sujeitos. Disponível em <http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm>. Acesso em 16.01.09 às 21:29hs.

adolescentes são vítimas diferentes, e expostas a riscos diversos e de modos diversos, na rede mundial de computadores, especialmente no que concerne à suscetibilidade quanto à criminalidade.

Atrai-se a atenção para tal premissa pelo fato de que, apesar de estarem num mesmo conjunto de regramentos, quanto ao artigo 241 da Lei nº 8.069/90, há o mesmo tipo de crime pela exposição por fotografias, na Internet, de uma criança e de um adolescente. Isso porque ambas as condutas são graves, mas a vitimização da criança relata uma atitude de maior reprovabilidade, pois que não é comum que uma menina de 7 anos fotografe-se ou seja fotografada nua, em poses libidinosas ou provocativas, por não estar em estado de desenvolvimento compatível a tal ação. No entanto, a mesma exposição fotográfica por parte de uma adolescente de 17 anos não pode sofrer o mesmo tratamento, pois que, beirando a maioridade biológica, é natural que desenvolveu (ou está em processo de desenvolvimento) uma consciência sexual, uma curiosidade quanto ao próprio corpo e à própria imagem.

Não há dúvida de que ambos os fatos são reprováveis, não se está aqui justificando condutas ilícitas, porém, o bem jurídico violado quando da deturpação no desenvolver saudável de um indivíduo em situação peculiar como uma criança, implica em impactos de maior monta na sociedade e na célula familiar. Tanto é assim que há agravante específica no artigo 61, II, “h” do Código Penal, para ações que lesionam criança, fato que não ocorre quanto a adolescentes e, por conta do Princípio da reserva legal, não há que se admitir interpretação extensiva *in pejus*. Em contrapartida, não há equivalência em agravamento para vítimas adolescentes, que também terminam por prescindir de proteção penal em boa parte dos países desenvolvidos como já tratado, em leis que privilegiam reprimendas contra crianças (“*child acts*”).

Tais prolegômenos servem para se tratar dos aspectos da vitimização de tais elementos sociais. É de se compreender que ambos os segmentos da vida são de aprendizado maciço, de descobertas e de fragilidade. Contudo, há uma faixa de idade de alta suscetibilidade, de influências passivas, ou seja, de sensibilidade extremada e em que a construção do caráter se dá de modo mais intenso que é a da infância.

Por isso quando se trata de vítima jovem, há que se compreender que necessária se faz

uma proporção quanto à capacidade vitimal de crianças e de adolescentes, que se mostra bastante diferenciada. Isso porque ao se atingir certas etapas de amadurecimento adolescente, os indivíduos passam a serem usuarios mais capazes de se auto-educarem sendo mais capazes de selecionar as companhias virtuais, os interesses na rede e, pelo interesse na tecnologia, dominar a linguagem e até mesmo a própria ciência da informática, tornando-se, em si, alvos mais difíceis. A criança, por sua vez, de regra necessita de navegação supervisionada, de programas de restrição de acessos a *sites* mais rígidos, e isso porque está mais tendente a ser influenciada pelos conteúdos acessados (que podem se dar indiscriminadamente) e pelos vitimizadores interessados (pedófilos ou simpatizantes).

Acredita-se que, enquanto o adolescente é capaz de rechaçar tentativas de vitimização com maior eficiência, a criança mostra-se alvo fácil especialmente por acreditar em histórias, fantasias e promessas, e não ter maturidade suficiente para perceber riscos com antecedência e dar valor aos bens jurídicos informáticos.

Sabendo da fragilidade da idade, vitimizadores pornógrafos infantis utilizam-se de salas de bate-papo com tema infantil na tentativa de aliciar interesse sexual de crianças, muitas vezes oferecendo imagens ou presentes para conquistar a confiança das vítimas. Mostra-se, pois, a criança, por sua imaturidade, maior propensão a acreditar e confiar no interlocutor, assim suscetibilizando as influências negativas.

Porém, não se quer restringir à vítima infantil o raciocínio vitimológico. A influência da rede e a disseminação de material de conteúdo sexual gera influências em ambas faixas etárias, tanto infanto, como juvenil.

Nesse sentido a Internet mostra-se como um ambiente de alto potencial de influência quanto a seus materiais, pois que a criança e o adolescente que acessam esse ambiente e assistem seu conteúdo, aprendem, absorvem e acostumam-se. Há, todavia, materiais de boa estirpe e que auxiliam no desenvolvimento intelectual, levando ao incentivo e entusiasmo (inclusive jogos), e materiais inadequados para aquelas etapas da vida.

Como a anonimidade é característica fulcral do ambiente virtual, reina na rede o envio e recebimento indiscriminado de material pornográfico não quisto, o que leva a todos os usuarios, inclusive às crianças e adolescentes a tornarem-se tolerantes com certos materiais,

fato este que gera consequências graves.

Kymberly J. Mitchell, David Finkelhor e Janis Wolak, da Universidade de New Hampshire, desenvolveram um trabalho denominado “*A exposição da juventude a material sexual não desejado na Internet – uma pesquisa nacional de risco, impacto e prevenção*”³¹³ em que jovens entre 10 e 17 anos foram arguidos acerca de suas exposições à pornografia na rede mundial de computadores. A partir disso, descobriu-se que os principais meios que levam material de conteúdo indesejado aos olhos do usuário jovem são as buscas de Internet, as leituras de *email* ou o clicar em *links* contidos neles e, ainda, os programas mensageiros instantâneos e que os materiais são maciçamente, nudez, intercurso sexual e violência (sexual ou não). O resultado dessa exposição não desejada, de acordo com a pesquisa, é o desenvolvimento de uma atitude leniente quanto a incidentes de estupro e violência sexual. Pelos autores, “*Exposição repetida a pornografia de Internet não desejada pode cultivar a percepção da juventude acerca de uma realidade sexual de forma que suas ideias sobre sexo sejam enviesadas*”³¹⁴.

Com isso, é de se concluir que apesar de haver uma maior fragilidade quanto à criança no que se refere a acessos a materiais e contatos relacionais na rede, ainda assim o potencial de risco da rede, especialmente no que se refere à disseminação de pornografia, leva a uma preocupação no sentido de que alguém da vitimização no sentido de influenciar negativamente por exposição o menor de 18 anos³¹⁵, há também uma vitimização reflexa, de maior

³¹³ MITCHELL, Kymberly J., FINKELHOR, David e WOLAK, Janis. The exposure of youth to unwanted sexual material on the Internet - A National Survey of Risk, Impact, and Prevention. Disponível em http://www.unh.edu/ccrc/pdf/Exposure_risk.pdf. Acesso em 22.10.08 às 23:20hs.

³¹⁴ “*Repeated exposure to unwanted Internet pornography might cultivate youths’ perception of sexual reality in such a way that they have biased ideas about sex* “. The exposure of youth to unwanted sexual material on the Internet - A National Survey of Risk, Impact, and Prevention. Disponível em http://www.unh.edu/ccrc/pdf/Exposure_risk.pdf. Acesso em 22.10.08 às 23:20hs.

³¹⁵ Aqui é curioso notar que não há tipo penal que se propõe especificamente a punir atitudes de divulgação ou difusão de material inadequado no país, mas tão somente normas de natureza administrativa, o que imediatamente denota uma inadequada análise criminológica das possíveis repercussões de tais exposições. O Estatuto da Criança e do Adolescente (Lei 8.069/90) apresenta os seguintes artigos para reger possíveis informações inapropriadas por seu conteúdo adulto, todas de caráter administrativo somente: “Art. 78. As revistas e publicações contendo material impróprio ou inadequado a crianças e adolescentes deverão ser comercializadas em embalagem lacrada, com a advertência de seu conteúdo. Parágrafo único. As editoras cuidarão para que as capas que contenham mensagens pornográficas ou obscenas sejam protegidas com embalagem opaca. (...) Capítulo II Das Infrações Administrativas (...) Art. 252. Deixar o responsável por diversão ou espetáculo público de afixar, em lugar visível e de fácil acesso, à entrada do local de exibição, informação destacada sobre a natureza da diversão ou espetáculo e a faixa etária especificada no certificado de

intensidade até e de maiores implicações prejudiciais à segurança pública³¹⁶.

A VÍTIMA GANANCIOSA

Bastante se discute acerca da ganância como fator influenciador no cometimento de um crime, especialmente os patrimoniais da modalidade estelionato. Especialmente levando-se em consideração que este é um sentimento negativo e egoísta de alguém que busca ter para si grande quantidade de poder, em especial, o dinheiro, a ganância tende a transformar as atitudes dos indivíduos, que notando possibilidade de vantagem patrimonial agem com menor cautela, assumem maiores riscos e chegam a poder prejudicar outros para atingirem seu intento.

Tem-se que o ganancioso é aquele indivíduo que busca ativamente modificar a sua situação de fato, intentando a ascensão (social, econômica, ou outra) ou alguma vantagem estritamente pessoal. É, pois, ator participativo e influenciador das pessoas que o cercam no intuito de obter seus fins, e capaz de ponderar suas atitudes frente a seus objetivos. Tal capacidade de raciocínio ponderativo, ainda que se possa dizer consciente, fica parcialmente

classificação: Pena - multa de três a vinte salários de referência, aplicando-se o dobro em caso de reincidência. Art. 253. Anunciar peças teatrais, filmes ou quaisquer representações ou espetáculos, sem indicar os limites de idade a que não se recomendem: Pena - multa de três a vinte salários de referência, duplicada em caso de reincidência, aplicável, separadamente, à casa de espetáculo e aos órgãos de divulgação ou publicidade. Art. 254. Transmitir, através de rádio ou televisão, espetáculo em horário diverso do autorizado ou sem aviso de sua classificação: Pena - multa de vinte a cem salários de referência; duplicada em caso de reincidência a autoridade judiciária poderá determinar a suspensão da programação da emissora por até dois dias. Art. 255. Exibir filme, trailer, peça, amostra ou congêneres classificados pelo órgão competente como inadequados às crianças ou adolescentes admitidos ao espetáculo: Pena - multa de vinte a cem salários de referência; na reincidência, a autoridade poderá determinar a suspensão do espetáculo ou o fechamento do estabelecimento por até quinze dias. Art. 256. Vender ou locar a criança ou adolescente fita de programação em vídeo, em desacordo com a classificação atribuída pelo órgão competente: Pena - multa de três a vinte salários de referência; em caso de reincidência, a autoridade judiciária poderá determinar o fechamento do estabelecimento por até quinze dias. Art. 257. Descumprir obrigação constante dos arts. 78 e 79 desta Lei: Pena - multa de três a vinte salários de referência, duplicando-se a pena em caso de reincidência, sem prejuízo de apreensão da revista ou publicação. Art. 258. Deixar o responsável pelo estabelecimento ou o empresário de observar o que dispõe esta Lei sobre o acesso de criança ou adolescente aos locais de diversão, ou sobre sua participação no espetáculo: Pena - multa de três a vinte salários de referência; em caso de reincidência, a autoridade judiciária poderá determinar o fechamento do estabelecimento por até quinze dias”.

³¹⁶ Aqui podemos falar de uma vitimização terciária, em que toda a sociedade paga, de modo reflexo, pela vitimização de parte da classe de crianças e adolescentes, porquanto cria-se uma geração tolerante a violências sexuais e abscondidas, gerando indiferença quanto a certos valores. Nesse sentido, o efeito iatrogênico defendido por CÂMARA, Guilherme Costa, Op. cit. p.118 e a criação de um custo social por conta da vitimização por BERG, Sata E. Identity Theft Causes, Correlates, and Factors: A Content Analysis. In Crimes of the Internet. Pearson Prentice Hall, New Jersey, 2008, p. 241.

encoberta por ideias hedonistas ou de avareza.

Some-se à mesquinhez a falta de compreensão da existência e da importância dos novos bens jurídicos, além da dificuldade em aceitar os riscos da nova sociedade informacional e compreender-se-á a grande quantidade de estelionatos ocorridos na rede³¹⁷.

Apenas para título de exemplificação, em abril de 2008, a empresa *Infosecurity Europe* liderou uma pesquisa na cidade de Londres para demonstrar até que ponto a ganância das pessoas impacta no afastamento dos deveres de proteção e responsabilidade com os bens jurídicos informáticos. Para tanto, ofereceu-se um questionário a ser preenchido e foi oferecida uma barra de chocolate para que em troca os candidatos preenchessem o campo da pesquisa em que se pedia que o indivíduo escrevesse suas senhas pessoais de segurança utilizadas no sistema operacional, no *Internet banking*, na rede, etc. 45% das mulheres e 10% dos homens se dispuseram a fornecer tais dados em troca do doce. Na mesma pesquisa, foi dito que os candidatos que preenchessem o campo com nome e número de telefone poderiam concorrer a uma viagem à cidade de Paris. 60% dos homens e 62% das mulheres se dispuseram a oferecer tais dados³¹⁸.

Respeitadas as devidas proporções, os estelionatos virtuais utilizam de técnicas mais sutis e menos explícitas para conseguirem obter dos usuarios dinheiro ou informações que gerem crédito. O que antes ocorria através de cartas, correntes, golpes de bilhetes premiados, hoje ocorre a partir de telas *pop-up* de *sites*, *emails*, e com alarmante frequência, por mensagens de texto via telefonia celular.

Praxes como a de surgir uma tela informando que o usuario foi o milionésimo usuarios a acessar o *site* e ganhará um prêmio, falsas animações interativas de jogos, promessas de emprego com altos salários, raspadinhas virtuais, correntes que indicam que companhias

³¹⁷ A tecnologia da informação mostrou-se como representante de um espaço econômico de altíssimo potencial exploratório e com lucros de grande monta. Exemplo principal é o da empresa Google Inc., criada por dois estudantes de doutorado, Larry Page e Sergey Brin, da Universidade de Stanford em 1996 e que tem seu valor de mercado em mais de US\$ 85 bilhões³¹⁷. Por estes motivos, pela ampla capacidade de atingimento de diversos segmentos populacionais e pelo potencial comercial, a rede terminou por mostrar-se um ambiente propício para negócios, e oportunidades das mais diversas mostraram-se rentáveis. Assim, muitas das propostas e ofertas podem persuadir e despertar em usuarios o interesse em arriscar-se no intuito de obter lucros ou vantagens.

³¹⁸ Fonte: <http://www.infosec.co.uk/page.cfm/Action=Press/PressID=1071>. Acesso em 22.04.08 às 07:14hs.

telefônicas darão aparelhos celulares gratuitos com a divulgação de mensagens, falsos sorteios de prêmios ou participação em programas de televisão, essas são apenas algumas estratégias que visam explorar a ganância do usuário, no intuito de persuadi-lo a clicar nos *links*, ceder informações, enviar *email* ou até mesmo entrar em *sites*.

O que ocorre é que o a ganância termina por ser fator preponderante, especialmente à vítima de estelionato, por conta de sua raiz comercial. Nas palavras de Cezar Roberto Bitencourt:

“Comerciar é a arte de negociar, de tirar vantagem econômica do negócio ou qualquer transação que se realize; esse aspecto encerra um jogo de inteligência, de astúcia, uma espécie de brincadeira de esconde-esconde, donde resultou a expressão popular de que “o segredo é a alma do negócio”. Em outros termos, é normal, nas transações comerciais ou civis, certa dose de malícia entre as partes, que, com habilidade, procuram ocultar eventuais deficiências de seu produto para, assim, realizar um negócio mais lucrativo ou vantajoso”³¹⁹”

Por isso e a partir das ideias de Nelson Hungria de que haverá a fraude penal nos casos em que se notar que há ideia preconcebida de uma das partes envolvidas para a frustração do equivalente econômico, é que se busca apontar que nos delitos informáticos o vitimário, já sabendo da falsidade do produto, vantagem ou prêmio ofertado, ainda assim aproveita-se do interesse egoístico da vítima para obter vantagem patrimonial.

Erich Fromm apontou que a ganância é metaforicamente *“um fosso sem fundo que exaure a pessoa em um esforço sem fim para satisfazer uma necessidade, sem jamais atingir a satisfação”³²⁰*. Pode-se dizer que, sob um enfoque criminológico, a ação do estelionatário é certamente gananciosa pois este visa obter para si em regra uma vantagem patrimonial a partir de um ardil sobre outrem. Porém, para que tal estratégia dê certo, é fundamental que a vítima

³¹⁹ BITENCOURT, Cezar Roberto. Tratado de Direito Penal – Parte Especial – Volume 3. 4ª Edição. Editora Saraiva, São Paulo, 2008, pp. 229-230.

³²⁰ Conforme análise da obra *Escape From Freedom* em <http://webspace.ship.edu/cgboer/fromm.html>. Acesso em 11.12.08 às 15:58hs.

esteja predisposta e propensa a aceitar o golpe com algum grau de credulidade. Assim, para que uma história ou estratégia dê certo, um sujeito deve ser ganancioso (o vitimário) e o outro sujeito deve ser ainda mais ganancioso (a vítima) e aberto para, ouvindo a proposta, acatá-la. O mesmo mecanismo se dá no hipnotismo, em que o hipnotizador precisa, para que possa exercer influência no candidato à hipnose, que este esteja aberto e disposto a ter sua mente manipulada.

Dessarte, a vítima gananciosa deve ter interesse e acreditar que pode ser milionária da noite para o dia, jogar um jogo de graça, ganhar um prêmio sem qualquer participação em concurso. É necessário que a vítima, antes de mais nada, tenha um sonho possível em sua mente, para que, uma vez alguém encontrando o veio a ser explorado quanto àquele desejo, explore-o para obter a vantagem.

A rede, com sua característica isoladora, simpática porquanto anônima, de personalidade moldável conforme o momento do usuário, é a principal ferramenta para a mobilização da pretensa vítima gananciosa.

Utilizando-se de divulgação de provocações e propostas em quantidade alta, com resultados baixíssimos, mas que se tendo em vista o número de usuários termina por ser considerável, bombardeia-se as caixas de correio com mensagens tentadoras como a de que dinheiro de parente distante foi descoberto e que é necessário somente o pagamento de uma falsa taxa para ser liberado ou o golpe do emprego na Nigéria que termina por exigir o pagamento do visto para obtenção de um emprego de gerência.

A questão é que parte da humanidade mostra-se essencialmente preguiçosa e prefere acreditar que há possibilidade de que a riqueza chegue a ela sem esforço laboral. Por isso, na esperança de receber um presente ou enriquecer, terminam por tornarem-se vítimas fáceis (torpes?), corrompidas por seus próprios desejos, e que, por isso, contribuem esperançosamente e de modo avaro para a consecução dos fulcros do vitimário. O estado de ganância, portanto, serve como facilitador para a execução dos crimes informáticos que se utilizam do argumento do prêmio, da troca, do brinde ou do grátis para, aleatoriamente, atingir seus alvos.

A VÍTIMA CURIOSA

Não há que se confundir as figuras da vítima ignorante e da vítima inocente/curiosa. Enquanto que a primeira sofre com ações que exploram sua vulnerabilidade técnica ou sua incapacidade de compreender a tecnologia e seus riscos, a vítima curiosa pode não ter vulnerabilidades em tais áreas.

A capacidade que a rede mundial de computadores tem no que se refere à quantidade de conteúdo de longe superou as pretensões da biblioteca de Alexandria. Ainda que certamente sem qualidade em todas suas esferas, a rede mostra-se um portal de infinitas informações a partir da janela de exploração que é a tela do computador³²¹. Não há como crer-se que alguém pode tornar-se um internauta sem uma veia exploratória, um interesse por informações e curiosidade.

Porém, há curiosidade no sentido de questionamento comportamental em busca de aprendizado e compreensão de mecanismos e sentidos e há a deturpação da curiosidade em graus de ousadia irresponsável. Pode haver a curiosidade quanto ao perigo, mas os limites da preservação da vida e da integridade física prevalecem e mesmo são impostos pela sociedade de modo mais ou menos moderado.

Porém, em alguns casos e quanto a alguns bens jurídicos de menor guarida pública, a restrição de acesso não ocorre, cabendo aos particulares controlarem suas próprias atitudes e aceitarem as consequências de tanto. O fim da censura e a capacidade de divulgação da Internet fez com que ideias como a do *Index Librorum Prohibitorum* da igreja católica fosse uma realidade distante. A curiosidade das leituras perdeu a restrição com a ampliação dos canais de jornalismo e comunicação, imprensas das mais diversas e popularização da leitura, propagação de religiões alternativas, fazendo com que a última lista dos livros proibidos pela igreja católica fosse publicada somente em 1948³²².

³²¹ Daí nomes de programas populares como “windows” (janelas) e “Internet Explorer” (explorador da Internet), entre tantos outros.

³²² A lista mais recente pode ser acessada pela rede através do site <http://www.cvm.qc.ca/gconti/905/BABEL/Index%20Librorum%20Prohibitorum-1948.htm>. A lista de 1559 em que se apresenta restrição às leituras de Martinho Lutero (Bíblia cum recognitione Martini Luteri, por exemplo) encontra no site <http://www.aloha.net/~mikesch/ILP-1559.htm#Bibles>. Ambos acessos em 11.11.08 às 03:06hs.

Exceto em países como a China que proíbe pornografia de qualquer gênero³²³, Japão que penaliza a exibição dos órgãos genitais, além das restrições havidas nas legislações árabes e muçulmanas, grande parte da civilização tem acesso amplo a multimídias sobre sexualidade, cabendo ao adulto buscar as informações que mais lhe pertinem ou interessam.

Conforme já dito em outro momento desta dissertação, alguns países do mundo dão aos indivíduos a liberdade de participarem de jogos de azar, mesmo que somente por curiosidade, fato que nosso país proíbe desde 1942 com a Lei das Contravenções Penais.

A rede mundial tem sua arquitetura aberta desenvolvida para permitir liberdade de circulação e acesso informacional. Exceto a China que restringe o trânsito de informações³²⁴, de regras a velocidade das conexões por banda larga, os programas de troca de dados como os *torrents* e a comunicação instantânea por comunicadores fazem da rede um ambiente de fácil troca.

Há, porém, dentre muitos dos usuarios, aqueles que apresentam curiosidades mórbidas³²⁵, abstratas ou ainda de índole sexual (*bycuriosity*) ou de lucro. Com exceção das duas últimas, já tratadas em itens específicos, o que se nota é que no intuito de aplicação de golpes virtuais, contaminações por códigos maliciosos ou programas espiões ou, ainda, para obtenção de informações valiosas, delinquentes virtuais utilizam-se da fraqueza humana (chamada de síndrome por alguns³²⁶), com muita ênfase na curiosidade mórbida como

³²³ Vide recente determinação do país em censurar, entre outros sites, o Google e Baidu, ambos buscadores, por falharem no controle de censura de conteúdo inapropriado que poderia ameaçar a saúde mental e física dos jovens. Disponível em <http://epocanegocios.globo.com/Revista/Epocanegocios/0,,EDG85809-16628,00-GOOGLE+E+BAIDU+NA+LISTA+DOS+WEBSITES+VULGARES+NA+CHINA.html>. Acesso em 16.01.09 às 21:44hs.

³²⁴ Os usuarios da rede desse país são obrigados a assinar documentos em que se comprometem a não acessar sites de conteúdo restrito pelo governo, sob pena de punição penal e, desde 2005, os blogueiros foram obrigados a se cadastrarem no governo para que suas postagens pudessem ser filtradas. <http://slate.msn.com/id/2122270>. Acesso em 11.11.08 às 03:01hs.

³²⁵ Aristóteles disse em suas poesias que “*nós gostamos das imagens mais precisas de coisas cuja visão é dolorosa a nós (...)*”. Trecho acessável no livro *Values and Virtues: Aristotelianism in Contemporary Ethics* de Timothy D. J. Chappell, publicado pela Oxford University Press, 2006. Acesso parcial em http://books.google.com.br/books?id=troG5dnqRLkC&pg=PA114&lpg=PA114&dq=enjoy+contemplating+the+most+precise+images+of+things+whose+sight+is+painful+to+us+source=bl&ots=JJWaRHrRb5&sig=7j728xF0Fte4uUMgWFD5WWfIQ8&hl=pt-BR&sa=X&oi=book_result&resnum=1&ct=result. Acesso em 11.11.08 às 03:21hs.

³²⁶ *Trainwreck Syndrome* é nomenclatura encontrada na psicologia para tratar da curiosidade mórbida, significando a síndrome do desastre, que faz com que o indivíduo se interesse por presenciar ou ver imagens de tragédias em que há morte de semelhantes ou de animais.

armadilha para atrair usuarios e fazê-los clicarem em pretensos *links* que prometem vídeos ou imagens de acidentes, catástrofes, corpos ou até mesmo ferimentos ou outros retratos degradantes do ser humano³²⁷.

O que nos cabe é o questionamento acerca de até que ponto pode uma curiosidade (ou ainda, uma síndrome) influenciar nas condutas preventivas além dos limites aceitáveis, a ponto de afastar a responsabilidade do usuario que conhece os riscos da rede que entende a alta potencialidade de vitimização da isca mórbida. Também, é de se entender que pode haver um verdadeiro limite patológico para a ação da vítima em tais casos, que pode ser considerada, de algum modo, irresponsável pelos fatores subjetivos do *iter victimae*, o que abriria a possibilidade de a criminologia atentar-se verdadeiramente a uma imputabilidade de vitimização.

³²⁷ São exemplos bastante recentes os de emails e sites que prometiam fotografias da menina Isabella Nardoni e da garota Eloá Cristina Pimentel, além de repetidos casos de fotografias de acidentes aéreos como o do grupo musical Mamonas Assassinas. Exemplos: <http://www1.folha.uol.com.br/folha/informatica/ult124u458347.shtml>, <http://blog.teteraconsultoria.com.br/2008/04/perfil-falso-orkut-isabella-nardoni.html>, <http://www.supranet.com.br/portal/v3/noticia.php?id=v29YFpmEBCabWgF>. Todos acessos em 11.11.08 às 03:32hs.

AS VÍTIMAS FRENTE AOS DELITOS INFORMÁTICOS

Não há dúvidas de que o vitimizador não escolhe seu alvo ao acaso. Pode-se dizer que três são os elementos amplos categorizadores de vítimas³²⁸: (i) ou se busca a vítima a partir de um perfil de pessoa; (ii) ou se busca a vítima a partir de um objeto de interesse de algum modo direta ou indiretamente em seu poder; ou (iii) ou busca-se a vítima pelo local em que ela frequenta. É, pois, a vítima, um sujeito de foco adequado, um alvo que se mostra preferencial seja por quem é, por como se porta, por o que possui ou por onde está.

Conforme exposto, a rede mundial de computadores mostra-se um ambiente propício constantemente para a execução de delitos informáticos, especialmente porque sua estrutura propicia a oportunidade, no sentido de que a contemporaneidade por si só traz a vítima para o ambiente e a vulneraliza. A soma de tal fator com a espécie de crime almejado pelo usuário mal intencionado e, ainda, com a contribuição do usuário que, negligente ou imprudentemente se porta, faz com que crimes determinados mostrem-se mais fáceis de serem cometidos a partir de certas condutas das vítimas.

Isso faz com que a potencial vítima dos delitos informáticos seja diferente das outras vítimas comuns, primeiro pelo fato de que o mero uso da Internet faz a criminalidade possível por si só; logo, conectar-se é ir em direção do perigo por si só. O segundo elemento da autovitimização estaria na ideia de que, diferentemente dos delitos comuns em que cada indivíduo pode eleger formas de se proteger e resguardar (por exemplo indo para a escola acompanhado, contratando um segurança ou até mesmo trancando as portas – elemento guardião ou *guardian*), no delito informático não há mecanismo perfeito de proteção e cada usuário ainda assim o utiliza, mesmo consciente de que há uma inefetividade da ideia de proteção total potencializada por posturas incorretas de usuários. Assim Raymond Cox III, Terrance A. Johnson e George E. Richards quando apresentam que:

“O problema central em policiar a Internet está no fato de que não é possível trazer outros humanos conosco. Não importa o quão sofisticados e complexos os ‘policiamientos’ para os usuários da

³²⁸ Cohen e Felson, 1979 *apud* SCHMALLEGGER, Frank e PITTARO, Michael. Routine Activity Theory and Internet Crime. In Crimes of the Internet. Pearson Prentice Hall, New Jersey, 2008, p. 304.

*Internet são, ainda assim serão todos dispositivos mecânicos. E não são reativos. São elaborados para prevenir ações que já foram identificadas. Não conseguem responder a novas intrusões e atividade criminal.”*³²⁹

Obviamente sem qualquer pretensão de esgotar as espécies de condutas existentes no que se refere aos delitos informáticos, decidiu-se por detalhar algumas delas no que se refere à forma de cometimento do fato típico frente à vitimodogmática. Isso porque há que se destacar o fato de que por mais que se defenda um Princípio de responsabilidade, um Princípio de autoproteção, a ideia de papel social da vítima e a existência da autocolocação em risco, ainda assim é de entender que há casos em que tais raciocínios se aplicam e outros que não, e, nos que se aplicam, a casuística mostra-se imprescindível para o correto entendimento do desenrolar da situação, notadamente pelo fato de que tal criminalidade recicla-se constantemente e modifica suas práticas.

A VÍTIMA DA INTRUSÃO INFORMÁTICA

Conforme já houve a oportunidade de dizer, a intrusão informática é uma forma de ingresso na máquina ou de acesso a programa ou serviço de titularidade de um usuário, sem que sua permissão tenha sido dada.

É importante que se trate da diferenciação das modalidades de cessão de informações que permitem acesso: há cessões lícitas e ilícitas.

No que refere as lícitas, duas são as formas de autorização possíveis no universo informático: a expressa e a implícita. A primeira seria a autorização dada pelo próprio usuário detentor do acesso que, ao passar (ele mesmo) pelos procedimentos de acesso seguro (geralmente através do binômio nome e senha), permite que, a partir de seu *login*, alguém utilize, em seu nome, um aparato ou um aplicativo. A segunda, por sua vez, se dá nos casos

³²⁹ “The central problem in guarding the Internet is that there are no other humans we can bring with us. No matter how sophisticated and complex the ‘guardians’ for the users of the Internet are, these are all mechanical devices. They are reactive. They are designed to prevent actions that have already been identified. They cannot respond to the new intrusions and criminal activity”. COX III, Raymond W. *et al.* Routine Activity Theory and

em que o usuário detentor titular do acesso, ao invés de proceder ao ingresso superando os mecanismos de segurança, fornece a um terceiro as informações necessárias para acesso, permitindo, também, que utilize dos serviços como se ele fosse.

No primeiro caso, foi o usuário quem acessou o sistema e, então, permitiu o uso. No segundo caso, um terceiro, em posse lícita dos dados para acesso – garantido pelo titular – ingressa como se o usuário oficial fosse. Ambas condutas, pois, não podem ser consideradas intrusão propriamente dita.

Contudo, ainda resta a modalidade ilícita, que também admite duas modalidades de acesso: o acesso por obtenção ilegal de informações de segurança e a intrusão por invasão de sistema ou quebra de mecanismos de segurança (*breakage*), resultando em acesso ilegal.

Quando se pensa a invasão por contorno ou destruição de mecanismos de confidencialidade de dados como, por exemplo, senhas, criptografia ou até mesmo mecanismos de restrição de acesso por controle biométrico, está-se tratando de vítimas com alta capacidade técnico-informática. São *crackers* capazes de, a partir de seus conhecimentos em programação, falhas de segurança e até mesmo por desenvolvimento de programas, sobrepujar os mecanismos de controle de acesso numa espécie de superação ou rompimento de obstáculos. Certamente, se possuem conhecimento acima da média e dominam a tecnologia, nenhuma ação de uma vítima leiga será capaz de impedir o sucesso de sua empreitada. A relação vítima-vitímario é, pois, irrelevante para nosso estudo, vez que o delinquente age diretamente da máquina, prescindindo de seu detentor, exceto no que se refere à manutenção do aparato ligado.

Assim, fica com especial destaque o acesso ilícito proveniente da obtenção ilegal das informações de segurança e não por meio de conhecimento informático avançado. Isso porque a grande maioria de tais obtenções é feita por mecanismos de engenhosidade social, restando também algum espaço para a obtenção a partir de códigos maliciosos também, mas que será analisado em seguida, nas ações de contaminação.

É de se destacar que ao tratar-se da intrusão, lida-se com uma ação de ingresso ilegal

sem necessariamente que haja qualquer consequência futura como a obtenção de números de cartão de crédito ou uso do acesso para prática de crimes como por exemplo, contra a honra. Destarte, é a intrusão o ato de violação do bem jurídico segurança informática imediatamente na modalidade confidencialidade e, sequencialmente, caso haja alterações de acesso ou arquivos, respectivamente da disponibilidade e da integridade. É portanto, o bem jurídico segurança informática o objetivo final da atividade.

O que ocorre é que em grande parte das vezes a forma da qual o vitimário se vale para obter o acesso não é técnica, mas sim ardilosa. A engenhosidade social, também denominada criatividade do criminoso, é utilizada para a obtenção de dados sigilosos de maneira bastante intensa. Há, pois, manipulação, por conta de alto índice de êxito em tal estratégia nos crimes relacionais ou em que se pode ter no relacionamento o mecanismo para sucesso.

Kevin Mitnick, considerado um dos principais *hackers* algum tempo atrás e hoje presidente de uma empresa de segurança digital nos Estados Unidos da América do Norte (*Mitnick Security Consulting, LLC*) escreveu em um de seus livros que o melhor modo de se obter informações sensíveis de uma pessoa, sejam ou não sigilosas, é perguntando diretamente a ela, tais dados³³⁰.

Essa realidade faz com que os delinquentes da rede sirvam de golpes que se utilizam mais de histórias convincentes, com alguma capacidade de persuasão, do que elaboradas e arriscadas estratégias.

Os ardis virtuais, ou *scams*, mostram-se como a principal forma de obtenção de informações capazes de levar a uma intrusão informática. Por isso, a vítima termina por ceder dados sem qualquer resistência quando, exemplificativamente recebe telefonemas de pessoas que se identificam como funcionários do provedor de serviço ou de seu banco. Certamente que de posse dos dados facilmente obtidos, conseguirão os delinquentes obter os intentados acessos aos meios, obviamente após indução ardilosa a erro do usuário cedente.

Por mais que os contratos (eletrônicos ou não) de serviço (disponíveis para leitura do usuário) apresentem cláusulas tratando da pessoalidade e da intransferibilidade de senhas, por

³³⁰ MITNICK, Kevin D. e SIMON, William L.. A Arte de enganar – Ataques de *Hackers*: Controlando o Fator

mais intensos e constantes que sejam os avisos, ainda os usuarios permanecem cedendo tais informações. A vítima, que talvez por desconhecimento quanto ao valor dos dados e quanto às infindas possibilidades de prejuízo por conta de acesso a suas informações, termina por dar reduzida importância às informações que levam à intrusão, e então fica mais suscetível a cedê-la. Também, por acreditar em argumentos de autoridade, mensagens aparentemente oficiais e timbres e cabeçalhos, o usuario de tecnologias confia em seu interlocutor e, desta forma, termina por dar a ele a chave para acessos que normalmente não daria, caso desconfiasse da intenção de qualquer atitude na sociedade de risco representada pela rede mundial de computadores.

Há, também, os casos de usuarios que terminam por ceder suas informações sensíveis por omissão. São as hipóteses em que senhas e nomes são anotados em papéis, cadernos, agendas, *post-its*, armazenados em programas de organização de senhas, anotadas no celular, entre tantas alternativas, podendo ser encontradas por quaisquer passantes. Do mesmo modo, a vítima, em não sendo diligente na salvaguarda de dados (por desídia, por otimismo, por crer que jamais será vitimizada, etc), termina por deixá-los disponíveis para que alguém garanta acesso.

O mesmo ocorre com as caixas de diálogo de alguns *sites* em que se vêem os dizeres “lembrar minha senha” ou as opções adotadas pelos navegadores (e até por alguns sistemas operacionais), no mesmo sentido, através de *cookies*. A possibilidade de um usuario mal intencionado que acesse o *site*, sistema ou programa utilizar-se do acesso para violar a segurança informática é latente. Por praticidade ou desinteresse em digitar a senha em cada acesso, o usuario expõe-se ao risco de seu bem jurídico ser violado.

Ainda, há a problemática da criação de sequências óbvias de numerais para proteção dos dados mais importantes; deve-se também levar em conta que quando a segurança traz grau razoável de complexidade, muitos usuarios, no temor de perderem o acesso, anotam suas senhas em locais de fácil acesso, permitindo que sejam encontradas.

A intrusão informática não pressupõe que, além do ingresso sem autorização, ainda incidirá o vitimário qualquer outra conduta; contudo, a mera leitura, cópia de arquivos e até

mesmo o acesso a pessoas ou informações sucessivas a partir de tal ingresso pode gerar consequência prejudiciais. Acredita-se que, enquanto há hoje lacuna legal quanto ao mero ingresso desautorizado em sistemas informáticos, provavelmente por conta de se dar valor baixo às consequências dessa conduta, em regra tais atitudes são o início de diversas práticas consequentes. A doutrina espanhola já propôs que o ingresso desautorizado fosse equiparado a uma invasão de domicílio mediante uso de chave falsa e até mediante o rompimento de obstáculo³³¹. Não é esta a verdadeira solução porquanto o bem jurídico lar não deve ser assemelhado ao bem jurídico segurança telemática que pode trazer muitas outras consequências diversas.

Acredita-se, também, que quaisquer crimes seguidos a uma intrusão informática merecem sofrer causa de aumento de pena, exceto nos casos em que o dever de proteção da vítima foi omitido, negligentemente, apesar de ser conhecimento de suas obrigações. As vítimas, em tal caso, seriam as ignorantes em algum aspecto, as inocentes e até mesmo as gananciosas.

A VÍTIMA DE CONTAMINAÇÃO POR CÓDIGO MALICIOSO

A contaminação por *malware* ou código malicioso tem diversas naturezas e pode ocorrer pelo uso dos mais diversos programas e com uma pluralidade de objetivos. Também, a contaminação pode se dar de muitos modos diferentes com ou sem a contribuição da vítima.

Em momento anterior, já se apontou os principais tipos de *malware* (vírus, *worm*, *rootkit*, *keylogger*, *trojan horses*, etc). Cabe-nos, aqui, demonstrar rapidamente os diferentes tipos de objetivos dos vitimários para, na sequência, demonstrar como se forma a relação com a vítima.

A contaminação por código malicioso pode ter os mais diversos fins: a obtenção de *login* e senha para acesso ao *email* ou outra conta alheias, a obtenção de dados bancários

³³¹ Estudo de Augusto Rossini sobre o projeto de lei nº 84/99 resultou na proposta apresentada em seu livro em que consta a seguinte modificação no parágrafo 4º do artigo 159 do Código Penal: “§4º. A expressão “casa” compreende: I- qualquer compartimento habitado; II- aposento ocupado de habitação coletiva; III- compartimento não aberto ao público, onde alguém exerce profissão ou atividade; IV- sistema informático ou

visando desvio de valores da conta a partir do *Internet banking*, obtenção de números de segurança para acesso em redes sociais e comunicadores instantâneos a partir de outra titularidade, contaminação para tornar sistemas de empresas e governos lentos ou indisponíveis, destruição de dados de usuário inimigo, escravização de máquinas alheias e até mesmo o mero intuito de difusão de criação benéfica ou maléfica.

Outra consideração no raciocínio de objetivo da contaminação, também, é a que leva em conta a intenção do agente quanto ao alastramento dos danos. É interessante notar que duas são as possibilidades: pode haver a mera contaminação de uma máquina individual (crime que lesiona bem jurídico individual) e pode haver a contaminação com o intuito de alastramento e causação de dano difuso (e aqui o crime seria de ação penal pública incondicionada).

A atitude da vítima mostra-se de altíssima relevância quanto ao crime de contaminação e isso se dá pelo fato de que o ambiente informático é de grande interatividade e também pelo fato de que para que qualquer arquivo ingresse num dispositivo, inicialmente há um alerta em que se pede a autorização do usuário (ou permissão) para a continuação.

Dessa forma, é imprescindível que se entenda que, em regras e salvo nos casos em que haja vitimário com alto grau de conhecimento informático, é a vítima a primeira responsável por sua própria contaminação. Porém, é de se notar que nem sempre a vítima conhece os riscos que corre em procedendo à aceitação da instalação de arquivos, nem sempre tem em seu aparato programas que a precavém, e, não raro a vítima é persuadida a aceitar o arquivo, pois que induzida a erro.

Contágios de códigos maliciosos costumam ocorrer a partir de *emails* com anexos infectados (ou mesmo cavalos de tróia), a partir de mensagens de cartões virtuais ou promessas de exibição de fotografias de algo chamativo, a partir de *downloads* de músicas, vídeos ou arquivos de áudio (que podem, inclusive ser *downloads* temporários a partir do *youtube*, por exemplo³³²), e até mesmo por programas conhecidos como *freewares*.

De todo o modo, na maior parte dos casos, precede ao contágio uma tela de advertência

telemático com acesso indevido ou não autorizado”. ROSSINI, Augusto Eduardo de Souza. Op. cit. pp. 238.

³³² Páginas Falsas do Youtube espalham vírus. <http://info.abril.com.br/aberto/infonews/102008/09102008-0.shl>. Acesso em 10.10.08 às 17:21hs.

em que o sistema, respeitando a interatividade, solicita que o detentor dos direitos de acesso determine suas ordens sobre as atitudes a serem tomadas pelo dispositivo (geralmente as alternativas à pergunta “aceita fazer o *download* do arquivo?” são “sim” ou “não”). A escolha do usuário em aceitar o *download* de um arquivo ou instalar um programa, deve sempre respeitar as bases de prevenção e cuidado no ambiente de risco, sob pena de gerar o contágio do dispositivo.

Em vezes, o vitimário maquia o código malicioso anexando-o em programas aparentemente inofensivos ou mensagens que exploram certas vulnerabilidades da vítima, como o famigerado vírus “*I Love you*” que disseminou uma praga na proposta de ser uma mensagem de amor, ou também as constantes mensagens falsas do SERASA ou Tribunal Superior Eleitoral e falsos envios de cartões virtuais, além de através de falsas ameaças como a de processos administrativos ou trabalhistas.

Neste ponto vale que se apresente o fato de que algumas ações produzidas pelo vitimário na tentativa de induzir a vítima a erro, frente à ideia da existência de um Princípio de autoproteção, devem ser consideradas evitáveis, e, outras, inevitáveis. Por isso, assim como no raciocínio de erros costumeiramente feito pela doutrina, na vitimodogmática, a ideia de ações escusáveis e ações inescusáveis devem ser vistas a partir de tal Princípio.

A informática desenvolve e evolui programas específicos que têm por intuito único o monitoramento constante das atividades perpetradas pelos usuários quando expostos aos incontáveis (e mutáveis) perigos trazidos pelos códigos maliciosos que constantemente transitam pelo ciberespaço. Antivírus, *antispywares*, *antiadwares*, limpadores de registros maliciosos, *firewalls*, detectores de intrusão, pacotes de atualização de sistema, *updates* de registros de *greywares*, todos são exemplos de programas com finalidade exclusiva de impedir que contaminações ocorram.

Porém, o fato é que os desenvolvedores de códigos maliciosos terminam por ser muito dinâmicos, constantemente desenvolvendo novos tipos de ameaças nesse sentido e isso faz com que a necessidade de aprimoramento e atualização constante de tais programas seja fundamental para que a proteção dos dispositivos verdadeiramente ocorra. De tal monta, o usuário informático passa a ter como dever básico o de proteção de seus conteúdos sensíveis,

lhe incumbindo a administração de seus aparatos e *softwares*.

Conhecendo a costumeira desídia no dever de cuidado da vítima, as empresas desenvolvedoras de programas de proteção tiveram por bem sempre apresentar a alternativa (e as vezes nem sequer a alternativa, mas sim a única opção) de os usuarios, ao instalarem tais aplicativos, terem automaticamente suas máquinas protegidas, pois que o próprio programa, sozinho, ao iniciar-se a conexão da rede, liga-se a um servidor para proceder à própria atualização e, de tempos em tempos, faz a varredura de toda a máquina na busca por ameaças de contaminação.

Mesmo assim, não raro os usuarios desativam as opções de segurança automática, dispensando as atualizações ou as interrompendo tão logo se iniciem, na pressa de seguirem para o objetivo almejado, crendo outrossim não serem alvos possíveis. Tal atitude comissiva deve ser compreendida como violação da responsabilidade vitimal de autoproteção.

A VÍTIMA DA VIOLAÇÃO DE EMAIL³³³

Afora as já argumentadas ideias apresentadas no que se refere à vítima de crime de intrusão informática, ou seja, as responsabilidades das vítimas no que se refere à proteção de seus dados cabendo-lhe escolha das senhas com algum grau de complexidade e distante de combinações relacionadas com números de registros do próprio usuario como RG, CPF e datas comemorativas, é de se destacar a necessidade de evitação da opção de o sistema ou os programas lembrarem-se da(s) senha(s) do usuario automaticamente (em especial em computadores acessados por terceiros ou computadores públicos), muito comum para os serviços de *email*.

³³³ O arquivado Projeto de Lei n.º 6.503/2006, de autoria da ex deputada Ann Pontes, procurou regulamentar esta matéria, alterando o artigo 151 do Código Penal, do seguinte modo: *PROJETO DE LEI No , DE 2006 (Da Sra. ANN PONTES) Altera o art. 151 do Decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal. O Congresso Nacional decreta: Art. 1º Esta lei altera o art. 151 do Decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal. Art. 2.º O art. 151 do Decreto-lei n.º 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação: “Art. 151. - Devassar indevidamente o conteúdo de correspondência real ou eletrônica fechada, dirigida a outrem: (...) §1.º(...) II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica, radioelétrica ou eletrônica dirigida a terceiro, ou conversação telefônica entre outras pessoas; ...” (NR) Art. 3º. Esta lei entra em vigor na data de sua publicação”.*

Porém, o ponto a se tratar quanto à vítima da violação de *email* não se refere àquela que, por conta de ceder seus dados de segurança por erro, voluntariamente ou por ignorância, termina por ter seu acesso ao serviço violado e utilizado. No caso, não se quer focar na confidencialidade do usuário, mas sim na violação do conteúdo da própria mensagem remetida.

As mensagens eletrônicas são enviadas por meio de pacotes de dados. Assim, qualquer arquivo é fracionado em diversas partes, e cada uma recebe uma numeração ordenadora para serem reagrupadas em seu destino. A operação de envio de pacotes é feita através da rede, que, por ser aberta e falível, remete tais pacotes diversas vezes, até que o dispositivo de destino envie de volta a informação de que a operação obteve sucesso. Isso significa que os dados são enviados diversas vezes, aproveitando-se do potencial descentralizado da rede, ganhando-se, assim, nos fatores tempo, eficiência e velocidade.

Porém, as mensagens enviadas (na realidade quaisquer pacotes de dados) são públicas e interceptáveis, podendo ser vistas por quaisquer usuários com conhecimento e interessados no conteúdo. Ronaldo Lemos Silva Júnior, inclusive, compara as mensagens remetidas na rede a verdadeiros cartões postais, com conteúdo visualizável por qualquer um³³⁴.

A partir de tais premissas, é de se dizer que a leitura de um *email* por parte de terceiros jamais poderia ser considerada violação de correspondência, e isso por dois motivos: o primeiro é pelo fato de que *emails* não podem ser considerados mensagens de conteúdo fechado e o segundo é pelo fato de o Princípio da Reserva Legal combinado com a Lei no. 6.538/78 fazer com que *emails* sequer possam ser considerados correspondência³³⁵.

Por isso, as recomendações basilares de proteção de conteúdo de mensagens são no sentido de focar-se em outros fatores de segurança como a criptografia e a esteganografia. Tais processos buscam codificar ou esconder uma mensagem fazendo com que uma eventual interceptação reste infutífera por ser, em si só, incapaz de permitir que o vitimizador obtenha

³³⁴ Em palestra proferida na Pontifícia Universidade Católica intitulada “Direito Informático”, promovida pelo Centro Acadêmico “22 de agosto” na Semana Jurídica de 2003.

³³⁵ *TÍTULO VI - DAS DEFINIÇÕES - Art. 47º - Para os efeitos desta Lei, são adotadas as seguintes definições: CORRESPONDÊNCIA - toda comunicação de pessoa a pessoa, por meio de carta, através da via postal, ou por telegrama.*

acesso ao conteúdo confidencial.

Neste sentido, é responsabilidade do usuário que quer certificar-se da confidencialidade de sua mensagem, que utilize de serviços e programas acessórios para garantir tal restrição, tendo-se em vista a própria engenharia da rede e o sistema de transmissão de pacotes. A desídia no que tange a tal obrigação faz com que eventual violação saia da esfera do Direito Penal, tendo-se em vista a negligência que contribui para o delito, remanescendo somente reparações em esfera cível³³⁶.

A VÍTIMA DO DANO INFORMÁTICO

Assim como na intrusão informática e na contaminação por *malware*, boa parte dos danos informáticos advém de ações dos próprios usuários vitimizados. Contudo, primeiramente parecem-nos obrigatórias algumas considerações quanto às peculiaridades de tais ações.

O artigo 163 do Código Penal, assim como o já apresentado artigo 155, ao tratar de furto³³⁷, aponta como objeto material da conduta que danifica o patrimônio a expressão substantiva “coisa alheia”. Contudo, é fundamental que se respeite, como já exposto, os Princípios da reserva legal, da taxatividade e do “*in dubio pro reo*”, que fazem com que interpretações extensivas e analogias *in malam partem* sejam vetadas.

Por tal motivo, houve por bem a criação do parágrafo terceiro do artigo 155 que expressamente equipara energia elétrica ou outra energia que tenha valor econômico como coisa móvel. Porém, até o momento – isso porque projeto de lei substitutivo³³⁸ de autoria do senador Eduardo Azeredo, em tramitação, propõe também que os dados sejam considerados coisas móveis por equiparação –, dados em si, por serem formados de *bits* e não átomos, são

³³⁶ Não trataremos dos sistemas de certificação digital que tem como função atribuir o correto caminho entre o envio e o recebimento de arquivos e mensagens a partir do monitoramento dos pacotes de dados adotado pelo Brasil porquanto este serviço almeja exclusivamente a fiscalização do envio de dados.

³³⁷ E também os artigos 156 (furto de coisa comum), 157 (roubo), 168 (apropriação indébita), 169 (apropriação de coisa havida por erro, caso fortuito ou força da natureza) e 180 (receptação), todos do Código Penal.

³³⁸ Substitutivo aos PLS 76/2000 (Autoria: Renan Calheiros), PLS 137/2000 (Autoria: Leomar Quintanilha) e PLC 89/2003 (Autoria: Luiz Piauhyllino).

mera linguagem e não possuem proteção penal equivalente.

Ainda assim, levando-se em conta que este trabalho almeja considerar as atividades dos delinquentes virtuais (não necessariamente criminosos, mas que cometem atos que violam de alguma forma direitos de usuarios) e das vítimas e suas condutas e respostas, há de considerar a conduta danificadora informática como relevante para estudo.

Remanesce a missão de esclarecer o que seria a danificação de um dado, tendo-se em vista sua imaterialidade e não se poder admitir a aplicação do artigo supracitado. Para tanto, a melhor estratégia é a busca pela etimologia da palavra dano, em seu sentido amplo. “*Damnum*”, palavra latina, significa a diminuição ou redução dos bens jurídicos de uma pessoa alheia por conta de uma ação ou omissão de alguém³³⁹.

Em nosso caso, os bens jurídicos tratados são aqueles referentes à segurança telemática, e, portanto, relacionados com a integridade, confidencialidade ou disponibilidade. Dano informático, pois, termina por ser a ação de modificar-se um arquivo, um programa ou um sistema, fazendo com que, por conta de tais mudanças, haja violação de qualquer dos bens jurídicos citados.

Diversas são as formas através da qual os dados podem ser danificados: por ações dirigidas especialmente a um arquivo, fazendo com que este fique corrompido ou alterado em seu acesso, não podendo ser lido, interpretado e reproduzido para seu usuario interessado; por modificações em programas específicos, levando a uma impossibilidade de acesso a determinados arquivos (intactos) a partir deste, exclusivamente; alterando as configurações do sistema levando-o a comportar-se de modo a que não mais se consiga atingir os fins ao qual é destinado (p. ex.: máquina que desliga automaticamente, sistema operacional que trava, erros de processamento de dados artificiais, etc.); efetuando-se alterações em aplicativos que geraria exposição de arquivos confidenciais, etc.

Portanto, qualquer alteração não autorizada e prejudicial, efetuada ou provocada indiretamente por alguém, em dados, e que impliquem numa diminuição dos novos bens jurídicos devem ser consideradas atitudes de dano informático.

³³⁹ DE PLACIDO E SILVA, Vocabulário Jurídico, V. II, Companhia Editora Forense, São Paulo, 1967, p. 472.

Ressalte-se que na toada dos anteriores raciocínios, o dano informático pode ser causado por códigos maliciosos que infectam a máquina, podendo, inclusive, servir como crime de maior gravidade e com maior pena, e que absorveria o crime de contágio por *malware*, mas agravaria sua represália. Também, importante que se compreenda que o dano informático pode ser causado a partir de ou como consequência de uma intrusão informática, ficando esta absorvida por aquela, que mereceria somente agravamento especial. Nas palavras de Danielle da Rocha Cruz:

“Antes de realizar uma sabotagem informática, o agente deve entrar em um sistema informatizado de dados, utilizando esse acesso como meio para a consecução de sua atividade final, que é alterar os dados ali contidos.”³⁴⁰

As intenções do agente, por sua vez, também admitem diversidade, pois que vão desde causar prejuízo informático para a vítima por vingança ou por intuito de sobrepujamento, quebrar códigos de segurança de arquivos confidenciais, a até mesmo aquilo que se denominou sequestro de dados (*data hijacking*).

No tocante à vítima, há – além das ideias preventivas já apresentadas quanto aos delitos de intrusão e contágio de códigos maliciosos – cuidados de especial valia e que servem tanto para evitar grandes consequências de um dano informático perpetrado quanto para prevenir seu acontecimento.

Usuarios que permitem acessos remotos por parte de outros – permissão para outro usuario controlar à distância sua máquina, a partir de uma conexão dedicada – além da falta de cópias de segurança de arquivos e configurações fazem com que a ação danosa termine por ter efeitos alastrados em grau muito maior do que o necessário.

Com isso, o que se quer apresentar é o fato de há uma parcela de dever de autoproteção da vítima quanto a seus próprios dados e configurações, devendo cada usuario não somente proceder à instalação de aplicativos de proteção e cuidado, mas também buscar o resguardo pós fato, ou seja, a precaução quanto à recuperação de dados eventualmente perdidos.

³⁴⁰ CRUZ, Danielle da Rocha. Criminalidade Informática – Tipificação Penal das Condutas Ilícitas Realizadas com Cartões de Crédito. Editora Forense, Rio de Janeiro, 2006, p.11.

Tal assertiva abre uma nova perspectiva para a interpretação da vitimodogmática, uma vez que, ao se pensar delitos informáticos, além de refletir o comportamento da vítima quanto à prevenção do fato – ou seja, atitudes que evitariam cometimento de crimes –, além de se avaliar a interação da vítima com seu vitimário no *item criminis/iter victimae* – a parêntese vitimal –, há também que se pensar na responsabilidade da vítima na evitação de resultados graves irreversíveis posteriores ao fato ou, ainda, na reversibilidade quanto aos efeitos da ação delincente.

Isso porque no meio informático a construção e manutenção do patrimônio virtual (composto de documentos, arquivos, programas, atualizações, senhas, evoluções, maturidades, etc) é de responsabilidade do próprio usuário. Também, pelo fato de que há riscos constantes quanto ao processamento de informações e seu manejo, não raro uma conduta alheia (ou uma ação do próprio usuário como proceder a uma atualização de sistema operacional) pode arruinar com os arquivos de dados do dispositivo.

O hábito, as características da rede e a necessidade, portanto, levam cada usuário a ser responsável por seus próprios dados e, uma vez tendo-os destruídos, corrompidos, modificados, fica responsável pela recuperação dos mesmos.

Em nossa perspectiva e a partir de tais pressupostos, não cabe ao Direito Penal punir com maior rigor a conduta do vitimário caso os danos informáticos sejam irreversíveis, pois que a reprimenda da conduta não poderá ser agravada por tal motivo, visto que ao usuário vitimizado cabe a capacidade de resgatar seus dados avariados a partir de sua responsabilidade de criação de arquivos cópias de segurança. Reversamente, do mesmo modo, não há porque se mitigar a punição ao vitimário do dano informático pelo fato de que o usuário possuía cópia de segurança dos arquivos e, pois, não sofreu prejuízo, pois que a segurança telemática em si merece a proteção, independente do tamanho do prejuízo sofrido pelo usuário.

A VÍTIMA DO SCAMMING

Assim como já explanado, o *scamming* é um esquema fraudulento, ou seja, uma fraude perpetrada através dos meios informáticos, no intuito de obter-se alguma vantagem ilícita, em

detrimento da vítima. Em outras palavras, o *scammer* é um estelionatário virtual, que se utiliza de armadilhas e golpes construídos com o intuito de obter aquilo que constitui a rede em sua essência e tem alto valor: informações, geradas a partir de dados, por sua vez, gerados por *bits* – a unidade virtual.

Não há limites para as possíveis formas para cometimento de estelionatos reais, assim como não o há para o cometimento através das tecnologias. Porém, a distância natural inerente à telemática faz com que arapucas possam ser cometidas explorando especialmente a receptividade vitimal representada por fraquezas humanas, sentimentos, lógica e até mesmo a ignorância, conforme apresentado em capítulo anterior. Além da potencialidade da rede no sentido de que sua abrangência e velocidade são insuperáveis, a frieza e anonimidade das informações que surgem nos dispositivos gera uma consequência interessante no sentido de que o usuário fica livre para, dentro de sua mente, criar a realidade (virtual) para aquilo que vê ou lê.

Assim como a leitura de um livro faz com que a imaginação do leitor voe livre, permitindo que este construa a realidade lida a partir de sua educação, valores, humor e até mesmo cultura, a troca de informações através da tecnologia traz a mesma possibilidade de interpretação. Certamente que a margem de interpretação existe especialmente quando o meio é o escrito, isso porque mensagens de vídeo, por exemplo, trazem consigo expressões, tons de voz, forma de expressar o sentido da fala e assim por diante.

O potencial imaginativo do usuário-alvo, então, chega a ser um viés de exploração do fraudador, que pode utilizar de sua criatividade para tentar atingi-lo, persuadindo-o a clicar em um *link*, receber um *email*, comprar um produto, instalar um *software* e assim por diante, dependendo do objetivo almejado.

Deve-se lembrar que o estelionato tipificado no “*caput*” do artigo 171 do Código Penal apresenta como finalidade do agente a obtenção de “vantagem ilícita” não restringindo-se à vantagem econômica, mas sim qualquer espécie, desde que implique em prejuízo para a outra parte.

O *scam* também pode ser denominado *phishing-scam* querendo dar o sentido de que há uma verdadeira pesca por vítima ludibriáveis pelo golpe e isso porque assim como num mar

em que há milhões de peixes e ali se navega, na rede há milhões de usuarios. Numa pescaria, lança-se uma isca e aguarda-se que o peixe a morda; no *scam*, lança-se o golpe por *email* ou *site* e aguarda-se que em algum momento, algum usuario gere o resultado pretendido. A obtenção do resultado é uma questão de tempo e paciência, pois que num universo virtual de quase um e meio bilhão de usuarios, a probabilidade de êxito é altíssima.

Porém, o estelionatário (*scammer*) não pesca com iscas lançadas ao acaso. Por haver o conhecimento (empírico ou lógico) de armadilhas que geram maior sucesso porquanto exploram fragilidades das vítimas e, por isso, funcionam com maior eficiência, os agentes escolhem e desenvolvem golpes com maiores chances de serem convincentes e levarem-no a obter números de cartão de crédito, informações pessoais, depósitos em conta corrente e assim sucessivamente³⁴¹. Há nítido meio fraudulento, pois que a indução em erro é latente.

Os golpeadores buscam arquitetar esquemas que gerem no usuario credibilidade, primacialmente. A ideia é convencer o internauta de que aquele *site* ou aquela mensagem enviada trata de um assunto verdadeiro e que há necessidade de atenção por parte do leitor, seja por conta da tristeza dos fatos – como em casos de *emails* que têm como anexo fotos de crianças doentes que teoricamente precisam de operação ou remédios caros e que, portanto, precisam de doações em dinheiro e a pedem – pelo fato de apontar uma oportunidade única para o usuario – o caso dos *gold bricks* –, por comunicarem um fato sério – como uma audiência criminal, uma dívida não paga ou uma encomenda de um pedido falso – ou até mesmo porque o *email* tem elementos que levam a crer serem de instituições sólidas e confiáveis – como bancos ou emissoras de televisão retratadas em *sites* idênticos aos oficiais.

A capacidade que os golpistas têm de criar novos golpes ou elaborar *sites* espelho (*sites* que aparentam ser de uma instituição mas na verdade são montagens) e explorar sentimentos como medo, tristeza, curiosidade, compaixão, dó, além de fragilidades como idade, ignorância, necessidades físicas ou médicas e inexperiência tem evoluído a cada dia, num exercício de criatividade que supera as expectativas. O nome dado para tais golpes que se utilizam da inventividade humana para criação de história ou situação que gere potencialidade fraudulenta é engenhosidade social, erroneamente denominada de engenharia social por conta

³⁴¹ Nesse sentido, sobre a teoria da oportunidade, COX II, Raymond *et al.* Routine Activity Theory and Internet

de o termo ter sido cunhado originalmente na língua inglesa (“*social engeneering*”) e que se refere à capacidade de influenciar atitudes e comportamentos sociais em larga escala.

De todo o modo, o agente, através de *emails* ou *sites*, gera na mente do usuário a crença de que deve abrir um arquivo anexo, baixar um programa, clicar num *link* ou fazer um depósito bancário levando-o a ter prejuízos das mais diversas montas.

O usuário que acredita que possui dívida em seu nome, ao receber um *email* de uma grande loja de departamentos acusando uma compra não paga, e que deposita o valor alegado na conta apontada ou imprime e paga o boleto bancário anexo na mensagem, em verdade está sofrendo o prejuízo por acreditar na história a ele contada sem perquirir sua veracidade e confiabilidade das informações. Há um prejuízo material que gera, obviamente, vantagem para o beneficiário do depósito. Do mesmo modo os *softwares* que são baixados de modo equivocado por indução em erro e que terminam por espionar a máquina alheia, copiando os números de cartão de crédito do usuário ou suas senhas, e os enviando para o agente, que, seguidamente, utiliza-os gerando vantagem. Também, é de se citar os *sites* espelho³⁴², normalmente de bancos, que, por sua similitude, acabam por fazer que o correntista ceda números personalíssimos e senhas diretamente para o estelionatário, que faz o desvio patrimonial em seu favor, por vezes comprando créditos de celulares ou adquirindo créditos virtuais (dinheiro virtual e que serve como moeda corrente para aquisição de bens reais).

Porém, há prejuízos experimentados nos crimes informáticos próprios puros que tratam de novos bens jurídicos e que se deve questionar acerca de haver ou não vantagem para uma parte e prejuízo alheio. Assim, se o golpe servir meramente para garantir acesso a um arquivo sem a autorização do detentor legítimo de direitos, imediatamente está-se diante de uma vantagem ilícita³⁴³. O mesmo é de se falar de estratégias para garantir acesso ao computador

Crime. Op, cit., p.310.

³⁴² Há um banco de dados de sites espelho no site <http://www.fraudes.org/showpage2.asp?pg=81>. Acesso em 18.11.08 às 13:10hs.

³⁴³ De acordo com Cezar Roberto Bittencourt, Heleno Fragoso defendia aposição de que a vantagem apontada pela lei seria exclusivamente a econômica porquanto está o artigo inserido no título de crimes contra o patrimônio. Se levada em conta tal posição, certamente que carece a legislação penal brasileira de tipo existente a ser adaptado para a realidade informática no caso de bens jurídicos de nova natureza. No mesmo sentido, Magalhães Noronha. Posição contrária, defendendo a generalidade da vantagem, do próprio autor, de Luis Regis Prado e de Guilherme de Souza Nucci. BITENCOURT, Cezar Roberto. Tratado de Direito Penal – parte especial 3 – Editora Saraiva. 4ª Edição. 2008, pp. 235 a 237.

alheio e, com isso, impedir o acesso do usuário legítimo a seus arquivos, programas ou à rede mundial de computadores e, ainda, quanto ao ardil para destruição de arquivo ou sistema alheios.

Importante é se levar em conta a inexistência de uso das informações obtidas para a geração de prejuízos de ordem econômica, exemplificativamente citando-se a obtenção de informações sensíveis sem que estas tenham uso prejudicial (contra a honra, contra a vida, contra o patrimônio); por conta de não haver tipificação de violação dos novos bens jurídicos em nossa legislação, em verdade não há tipo penal de estelionato e, em boa parte dos casos, qualquer tipificação.

Porém, é de se atentar para o fato de que ainda que os bens jurídicos fossem protegidos pelo ordenamento jurídico brasileiro, deve-se levar em conta que a vítima pode não dar valor a tais bens e, nesse sentido, dispor deles renunciando de sua proteção – seja com dolo, seja com culpa em sentido estrito –, levando o prejuízo a uma natureza lícita. Isso imediatamente torna legal e legítima a conduta violadora do bem segurança jurídica, assim, também, afastando a tipicidade da rubrica da fraude que taxativamente tem como elemento normativo do tipo a ilicitude.

A vítima do *phishing-scam* é certamente vulnerável em algum aspecto. Porém, cada golpe prima por explorar uma das formas de vulnerabilidade, de acordo com aquelas apresentadas acima. Em regra o vitimário não ganha por focar especificamente o golpe em um usuário, mas sim busca criar uma armadilha que tenha um mínimo de concisão para ludibriar o máximo número de pessoas possível. Há um ganho pelo volume de vítimas mais do que pela qualidade de uma delas; porém, todos os usuários atingidos, em verdade, apresentarão mesma vulnerabilidade (receptividade) no setor explorado dentre os já apresentados (dó, caridade, curiosidade, etc.).

A pessoa que termina por cair no golpe costumeiramente contribui com tal ato, pois que deixa de educar-se quanto às principais ameaças e fraudes da rede, habitualmente comunicadas por meio de jornais, revistas, e *emails* e através dos *sites* oficiais das empresas que terminam por ter seus logotipos e nomes utilizados indevidamente. Não raro os golpistas, para conseguirem obter sucesso, montam golpes logo em seguida de notícias de jornal

televisivo que geram impacto e interesse social, como desastres, sequestros, homicídios e assim sucessivamente.

Por conta disso, a correta educação contra *scamming* deverá buscar não demonstrar o tipo de estratégia utilizada ou o golpe desenvolvido somente, mas também a forma como o comportamento da vítima influencia o agir do delinquente. Assim, é de se publicar preventivamente que a montagem de um estelionato pela rede aproveita da falta de terceiros para auxiliarem a vítima a ponderar sobre o risco de certas atitudes, somado com a exploração das fragilidades. A dinâmica do desenvolvimento de golpes não pode ser acompanhada pelos meios de comunicação, vez que se modificam diariamente com velocidade alta. Para tanto, a compreensão da rede como sociedade de risco “*sui generis*” somada à compreensão dos espaços explorados pelos golpistas gerariam uma prevenção criminal de maior eficiência.

A VÍTIMA DO SPAMMING

Ao tratar do *spamming*, tem-se que levar em conta, inicialmente, não haver qualquer regramento penal pátrio criminalizador do envio de mensagens não solicitadas. Contudo, tendo-se em vista que alguns defendem a ideia de que o remetente das mensagens acaba verdadeiramente por produzir uma espécie de furto de tempo, ou melhor, termina por causar, por conta do acumulado de efeitos da prática, prejuízos de grande monta. Isso porque a quantidade de mensagens comerciais não solicitadas remetida por mensagens de texto ou por *email* (somada à falibilidade da tecnologia que ainda não filtra com segurança absoluta mensagens de destinatários legítimos com mensagens *spam*) obriga o usuário a perder, diga-se exemplificativamente, 30 segundos por dia no descarte de tal material. Ao final de 5 dias úteis, 2 minutos e meio foram perdidos. Ao final de um mês com 4 semanas, foram 10 minutos perdidos. Ao final de 6 meses, 1 hora perdida e em 4 anos, um dia inteiro de trabalho foi dedicado exclusivamente ao serviço de apagar mensagens comerciais, gerando prejuízo para o profissional liberal, para a empresa contratante dos funcionários, e até mesmo para a Administração Pública, todos alvos dessa prática.

Também conhecidos como ervas-daninhas informáticas, os *spams* de regra são remetidos indistintamente, a partir de um sistema de envio aleatório programado para

disseminar a mesma mensagem comercial para todos os endereços de *email* possíveis numa combinação de caracteres, ou ainda a partir de endereços eletrônicos adquiridos em bancos de dados.

No que se refere aos métodos de controle propostos, quais sejam os sistemas já explanados de *opt-in* e *opt-out*, são diferentes as vítimas de tais fatos. Assim, o envio de mensagens não solicitadas a partir de um sistema *opt-out*, ou seja, a remessa de *spam* para um usuário particular que optou para que cessassem os envios, viola um direito individualizável, portanto, o bem jurídico particular. Mas ao considerar-se o sistema *opt-in*, ao revés, acredita-se que a violação adquire um sentido coletivo, pois que a ação de opção de aceitação é pressuposto indispensável para qualquer remetimento. No sistema *opt-out*, permite-se a remessa de mensagens mesmo sem a solicitação, e é conduta do destinatário que determina o impedimento particular de recebimentos – é pressuposto a aceitação geral de todos os usuários. No sistema *opt-in* está o remetente impedido de difundir qualquer mensagem não solicitada, havendo o rechaço de toda a sociedade quanto a essa conduta – é pressuposto a negativa geral de todos os usuários. Por isso, ao desrespeitar o sistema escolhido *opt-in*, há bem jurídico coletivo atacado, enquanto que no outro sistema optado, individual.

Muito se discute se há relevância na conduta do usuário para ser vítima do *spamming* no Brasil, vez que não há ainda determinação de regramento e a maioria dos países rege administrativamente a conduta. Especialmente por não haver legislação determinando o modelo seguido pelo país, é a conduta da vítima determinante para tal ação.

Isso porque o principal interesse de um *spammer*, assim como o de uma empresa que distribui panfletos, é ter sua marca conhecida, seus produtos divulgados. Some-se a isso o custo praticamente nulo da divulgação por *email* e a estratégia de *marketing* compensa. Por isso, sempre que *emails* forem cedidos por usuários, sempre que houver a leitura das mensagens não solicitadas, e sempre que a partir de um *email* os usuários acessarem as páginas no anunciante, terá válido a pena a incômoda ação de divulgação.

Portanto, natural que o usuário destinatário das mensagens contribua muito para sua perpetuação, sempre que publica seus *emails* em blogs, bate-papos, fóruns de discussão, e mesmo em cadastros. Contribuem, também, quando demonstram que a publicidade trouxe

resultado, acessando as páginas virtuais dos fornecedores, e até mesmo, quando não acessam mas respondem à mensagem solicitando sua retirada do banco de dados de *emails* do anunciante ou ainda clicando na opção “se não deseja mais receber estas mensagens, clique aqui”.

Ora, se não há qualquer regramento ou punição para tais condutas, a resposta ou o pedido de cessação apenas servem para confirmar a validade comercial daquele *email* e isso, em verdade, estimula a continuidade e o crescimento das ações de envio de mensagens.

De sorte que há uma competência vitimal para a evitação de *spams*, desde em estabelecendo-se a obrigação de não se ler tais mensagens nem constar os *sites* remetidos, bem como em não responder, ler ou clicar em *links* que prometem cessação de envios. Recomenda-se, também, que se tenha um segundo endereço virtual destinado exclusivamente ao envio de *spams*, driblando-se, assim, a eficácia de tal prática, preventivamente desestimulando a difusão.

AS CONSEQUÊNCIAS DA ATITUDE DA VÍTIMA

Seguindo os ensinamentos apresentados sobre vitimologia, é de se concluir que o evoluir dos estudos demonstram com bastante convencimento que o estudo da vítima potencial, sua personalidade, seu momento de vida, sua educação e sua capacidade de prever riscos, a forma como compreende a realidade, e até mesmo os ambientes que frequenta são alguns dos fatores fundamentais que influenciam o cometimento de um delito e sua própria ecologia.

Indiscutível que partindo de pressupostos como os acima apontados, até que instintivamente, um criminoso real opta por assaltar a vítima mais frágil, mais fraca e mais baixa, prevenindo-se, assim, de reações adversas e cuidando para que sua ação traga o sucesso pretendido. Por vezes, também, escolhe o alvo, aproveitando-se do elemento surpresa para que, assim, evite que a percepção ou a intuição do futuro ofendido possam ser acionados e, com isso, afasta as possibilidades de variáveis defensivas aflorarem no *iter victimae*; certamente, com isso, utiliza-se de recurso que dificulta a reação da vítima numa ponderação planejada levando em conta que faz parte da ação delinquente conhecer aquele que sofrerá a ação.

Sabendo que o fato criminoso é composto de momentos que antecedem a ação, a ação propriamente dita e momentos posteriores, o delinquente não raro utiliza-se de métodos que evitam que sua identidade possa ser reconhecida num futuro, caso haja consequências.

É, pois, certo, que ações de vítimas têm imensa relevância para o aperfeiçoamento de um delito. Assim, a necessidade de se estabelecer uma política criminal com tal viés faz-se mister. Por política criminal, entende-se a ciência a partir da qual se analisa os procedimentos através dos quais a sociedade responderá ao fenômeno delinquente que traz a intranquilidade, buscando o melhor meio para manter certas condutas em limites aceitáveis, vez que normais³⁴⁴.

³⁴⁴ Nas palavras de Francisco Bueno Arus “*La maneira mas obvia y general de preocuparse por las victimas em uma fase preventiva es cuidarse de aplicar “políticas sociales, sanitarias (incluída la salud mental), educativas, económicas y políticas dirigidas especialmente a La prevención del delito com objeto de reduzir la victimización y alentar a las victimas que La necessiten” in La atencion a La victima Del delito. Actualidad Penal. Actualidad Editorial. Madrid. 1990. p.298*

Conforme já apresentado nos seus mais variados aspectos, a postura que cada usuário da rede toma, impacta diretamente em si mesmo, levando em diversos casos a atitudes de pessoas mal intencionadas. Isso se dá pelo fato de que dentre as importantes características dos delitos tratados, a interatividade dos sistemas informáticos faz com que boa parte das consequências do ciberespaço seja gerada por ações da própria vítima. Daniele da Rocha Cruz, neste sentido:

“Com respeito aos fatores que incrementam a vulnerabilidade dos sistemas informáticos, é importante dizer que as próprias vítimas contribuem indiretamente para o aumento da criminalidade informática. Esse fenômeno criminoso afeta vários tipos de vítima, tanto pessoas jurídicas como físicas”³⁴⁵.

Não se está com isso buscando isentar o vitimário da culpa por violar bem jurídico alheio, mas tão só precisar com maior justeza o conceito de que há um cruzamento lógico entre a atitude tomada pelos vitimados no ciberespaço e a atitude tomada pelo ofensor.

A tecnologia da informação, por mais que se defenda que goze da concepção de anonimidade, não foi construída para a impunidade. Não é verdadeira a afirmação de que a virtualidade é uma forma segura e impune de se cometer atos delinquentes. Isso se dá pelo fato de que a navegação, o acesso e o uso de programas deixam vestígios³⁴⁶ e, assim, admite a rastreabilidade daquele que se utiliza do meio ambiente especial.

Ocorre que expertos em informática conhecem e compreendem que ao navegar geram vestígios e, pois, tendem a buscar apagar tais traços dos dispositivos de registro, tornando sua navegação verdadeiramente invisível. Também, como a anonimidade, esse fato traz vantagens para o delinquente e desvantagens para a vítima pois que sendo rastreada passa a ser alvo mais propenso ao sofrimento de uma violação.

³⁴⁵ CRUZ, Danielle da Rocha. Op. cit. p. 15.

³⁴⁶ Aqui haveria que se discutir se seriam vestígios propriamente ditos os rastros virtuais registrados pelo ingresso em sítios, uso de programas e troca de mensagens. Tal debate poderia ser levantado pelo fato de que vestígios costumam ser interpretados como traços, rastros e indícios gerados normalmente pela presença física de alguém no local dos fatos. A questão da ubiquidade e da virtualidade, assim, gera novo questionamento tendo-se em vista que não há própria e necessariamente um local específico em que uma ação delinquente virtual tenha ocorrido. Contudo, temos que o melhor raciocínio seja o de interpretarmos a expressão vestígio em seu sentido amplo como qualquer material a partir do qual se consiga extrair uma prova que aponte para a materialidade e autoria de

Diz-se isto porque conhecendo as atividades comuns da rede, boa parte dos vitimários acaba por plantar simples mecanismos de rastreamento em *sites* de alta procura e de duvidosa segurança digital, criando-se uma espécie de emboscada em que o usuário por si só termina por clicar em algum ponto da tela e ele próprio infecta sua máquina com um programa que o identifica e informa ao vitimário cada passo da navegação.

Da mesma forma pode o ofensor criar códigos programados para lesionar o bem jurídico de outrem: programas que automaticamente se executam nos dispositivos alheios, mas que exigem do infectado permissão para que isso ocorra. Desta maneira, não raro criam os vitimários páginas com conteúdo erótico, com atrativos como fotografias de acidentes ou delitos, *links* que prometem levar ao *download* de músicas e que, em verdade, terminam por fazer com que o usuário instale em seu dispositivo o código malicioso.

Para que se possa raciocinar uma resposta consistente ao combate de delitos informáticos, inicialmente imprescindível que se estabeleça a linha que se toma para considerar a conduta da vítima.

Apregoa Cancio Meliá que quatro são as ideias a serem consideradas na construção dogmática do impacto do comportamento da vítima: a) o raciocínio da concorrência de culpas e de que há um dever objetivo de cuidado por parte de vítimas; b) a ideia de que a vítima deve ter assumido conscientemente sua postura e compreenda a extensão de seu consentimento; c) a diferença entre autocolocação da vítima em risco e heterocolocação da vítima em risco consentida; e d) o raciocínio vitimodogmático de merecimento de proteção estabelecendo-se o chamado “Princípio vitimológico” como critério de extensão de responsabilidade do autor, medindo-se a responsabilidade de autoproteção da vítima³⁴⁷.

A assunção de que há uma quantidade de responsabilidade por parte de todos os atores do crime, e que, assim como há a obrigação de pretensos e futuro vitimários em respeitar os bens jurídicos das vítimas, há a obrigação da pretensa e futura vítima de, em podendo, evitar ser alvo de violações, tomando as cautelas mínimas necessárias e evitando expor-se a riscos

um delito.

³⁴⁷ CANCIO MELIÁ, Manuel. *Conducta de La Víctima e imputación objectiva em Derecho penal – estudio sobre los ámbitos de responsabilidad de víctima y autor em atividades arriesgadas*. Segunda Edición. J. M. Bosch Editor, Barcelona, 2001, pp. 91-92.

excessivos e desnecessários.

Isso nos leva imediatamente à ideia de que descumprimento das obrigações de lisura social por parte de um indivíduo geram o direito-dever do Estado em puni-lo, aplicar-lhe uma pena e fazê-la cumprir de modo a evitar novo acontecimento semelhante de acordo com seu modelo penal. Qual deverá ser a consequência gerada, então, com o descumprimento (doloso ou negligente) da obrigação de um indivíduo em se proteger e evitar que violações a si ocorram?

O entendimento de que o descumprimento de obrigações e responsabilidade, violando o que se chama “Principio vitimológico”, gera uma atitude inadmissível por parte do vitimizado, consequentemente dando ao Estado alternativas: ou utiliza-se do incremento do risco causado pela vítima como fator determinante para a justa aplicação da pena, reduzindo o *quantum* de sanção aplicada ao vitimário, ou escusa-se da obrigação de punir, pois que diante de uma atitude que desmerecimento de proteção por parte da Administração Pública³⁴⁸.

Há, primeiramente, que se consirar os seguintes pontos para o raciocínio do âmbito de responsabilidade da vítima: primeiro, a atividade delinquente deve ter sido organizada conjuntamente entre autor e vítima; segundo a conduta da vítima não poderá ter sido instrumentalizada pelo autor – se a vítima não tiver base cognitiva para agir, não poderá ser considerada auto-responsável – e, terceiro, o autor não pode ter um dever de proteção específico frente aos bens da vítima.

Deste modo, para tratarmos do Principio vitimológico e de uma possível co-responsabilidade da vítima, o crime deve ser de relacionamento, a vítima não pode ter sido induzida a agir de certo modo e o autor não pode garante dos bens violados, sob pena de não se poder tratar de competência vitimal.

Certamente, para isso, deve-se mensurar o grau de consciência do vitimizado quanto à suas atitudes frente à violação. Uma vez reconhecido o aumento do risco consciente ou presumido, está-se frente a uma situação de inescusabilidade de atitude vitimal. Aqui cabe

³⁴⁸ Segundo Cancio Meliá, “*Dependiendo de esa valoración, La conducta de la víctima podrá disminuir La responsabilidad del autor o incluso excluirla por completo*” CANCIO MELIÁ, La exclusión (...), Op. cit. p. 467.

comentar a teoria da ação jurídica defendida por Bierling³⁴⁹ que aponta o fato de que bens jurídicos são juridicamente tutelados se e somente se o seu titular os considera e trata como bens de valor; por isso, imediatamente uma permissão de ofensa justificaria a desnecessidade do Estado em tutelá-lo juridicamente, o que reforça a ideia de um Princípio vitimodogmático.

Há, contudo, a partir do critério de Edmund Mezger quanto à teoria da ação jurídica, a necessidade de que o abandono seja consciente³⁵⁰, levando-nos, finalmente, a questão da heterocolocação da vítima em risco consentida que deve ser avaliada, pois que apesar de toda a diligência ou de sua consciência quanto ao limite admissível de risco assumido, ainda assim pode ela ser levada à situação delinquencial contra sua vontade e inevitavelmente.

Para melhor compreender tais ideias, acredita-se fazer-se mister o desenvolvimento das ideias de consentimento do ofendido e de autocolocação da vítima em risco, lembrando-se que o segundo instituto é característico da teoria funcionalista do delito.

CONSENTIMENTO DO OFENDIDO

O instituto em tela trata da situação em que, apesar da existência de um fato típico perpetrado por alguém, ainda assim afasta-se do Estado o poder-dever de punir porquanto demovida a antijuridicidade da conduta pela ação do titular do bem jurídico atingido que aceita a lesão, anuindo com seu cometimento.

Trata-se de causa supralegal de exclusão da reprovabilidade da ação, sem previsão no rol do artigo 23 do Código Penal brasileiro, mas que tem redação explicativa no código italiano de 1930, em seu artigo 50, que apõe que “*non è punível quem offende ou põe em perigo um direito, com o consentimento da pessoa que dele podia validamente dispor*”³⁵¹. Certamente

³⁴⁹ *apud* PIERANGELI, José Henrique. O Consentimento do Ofendido da Teoria do Delito. 3ª Edição revista e atualizada. São Paulo. Editora Revista dos Tribunais. 2001. p. 79.

³⁵⁰ E Welzel ainda acrescenta que deve, também, ser sério e corresponder à verdadeira vontade do consenciente, afastando-se a vontade do ébrio ou incapaz, ou que teve sua liberdade de escolha afetada por qualquer externalidade. PIERANGELI, José Henrique. Op. cit., p. 79.

³⁵¹ “**Art. 50 - Consenso dell'avente diritto** - *Non è punibile chi lede o pone in pericolo un diritto, col consenso della persona che può validamente disporne*”. Disponível em http://www.usl4.toscana.it/dp/isll/lex/cp_11.htm#L1t3c1. Acesso em 18.01.09 às 14:30hs.

tem relação direta com o Princípio da Disponibilidade a partir do qual certos direitos individuais admitem transação por parte de seus legítimos titulares e termina por seguir a lógica processual das espécies de ação penal classificadas pelo Direito Penal brasileiro, uma vez que admite que indivíduos disponham conscientemente de seus bens que somente possuem relevância para si, sem impactar na coletividade ou em direitos ínsitos.

O que se nota é que há um certo consenso na doutrina quanto ao fato de que os bens que admitem que o particular consinta com sua ofensa são em grande número aqueles de caráter patrimonial e personalíssimos, essencialmente disponíveis, e que não impactam em valores difusos sendo, pois, bens jurídicos que não se confundem com seus titulares mas sim a ele pertencem.

De modo geral, os delitos informáticos tipificados nas legislações penais estudadas impactam das duas formas nos bens jurídicos: tanto no que se refere a bens disponíveis quanto a indisponíveis.

No que se refere aos delitos informáticos, há que se refletir ainda a natureza dos novos bens jurídicos, uma vez que a segurança informática em sentido amplo, se considerada bem jurídico coletivo, mereceria a tutela penal independentemente de valoração, pois que inerentemente indisponível. Nossa opinião, porém, apesar de no sentido de que há a criação de uma nova espécie de meio ambiente, é a de que nem todos os interesses tutelados dentro da rede são coletivos, mas tão somente aqueles que geram impacto na sociedade informacional com capacidade de prejuízo coletivo.

Nesta linha de raciocínio, seriam indisponíveis os bens jurídicos atingidos por delitos informáticos de pornografia infantil, ataques ciberterroristas, clonagem de cartão de crédito, *spamming*, *scamming* coletivo, inserção de código malicioso com potencialidade de contágio subsequente, apologia ao crime ou criminoso e incitação ao crime e crime de exploração de jogos de azar. Nesses casos, sempre o bem jurídico ou será autônomo quanto à informática e já protegido por ações penais públicas incondicionadas, ou terá relação com a segurança informática com potencialidade de alastramento e impacto em múltiplos usuários. Violar a disponibilidade, a integridade ou a confidencialidade de sistemas de acesso público ou governamentais por certo atinge bem coletivo.

Contudo, certas condutas como as de intrusão informática, “furto” de identidade, inserção de código malicioso (sem disseminação sequencial), crimes contra a honra, *scamming* individual, interceptação de *email*, violação de direito autoral e ainda ameaça e extorsão informática podem ter como alvo um bem jurídico já explícito na ordem penal ou a segurança telemática e podem ter incidência e potencial de prejuízo exclusivamente individual. De todo o modo, os bens jurídicos terminam por serem disponíveis ou aqueles que merecem proteção penal somente por ação penal privada, dando característica de possibilidade de haver a violação consentida.

É de questionar se há como adaptar a ideia de consentimento do ofendido com o ambiente *sui generis* que é a rede mundial de computadores. Isso porque a grande parte dos delitos perpetrados na rede ocorre sem o conhecimento direto do usuário vitimizado que termina por ter seu sistema invadido, informações sensíveis lidas e até mesmo seu sinal utilizado de modo mascarado gerando, portanto, prejuízo por causa uma conduta que parte de um agente delinquente. Haveria a possibilidade de se entender que ao não tomar as cautelas necessárias (e conhecidas) para a segurança de seu sistema informático, a vítima terminaria por consentir indiretamente com a conduta prejudicial a si mesma?

Em realidade tem-se que não. Para que se configure o instituto em tela, não basta exclusivamente que o bem jurídico seja disponível. No caso supra, se trata de uma intrusão informática com a finalidade única de vencer as barreiras da segurança do dispositivo de determinado usuário, se está diante de uma violação ao bem jurídico particular que é, por exemplo, um computador e que teve somente os dados de um determinado indivíduo lidos.

Certamente que pode qualquer usuário consentir que alguém tente invadir o sistema de seu dispositivo; contanto, na maioria dos casos em tela o que se tem é que, por um descuido, omissão ou até mesmo negligência de um indivíduo, e há uma violação de seu bem jurídico. Haveria de se falar em consentimento culposos ou inconsciente? De acordo com a doutrina, não basta que o direito seja disponível e seja exercido por seu titular para que se configure o consentimento. Isso porque uma pessoa que possua uma jóia e seja ameaçada com uma arma de fogo entrega ao assaltante o bem, dispondo-o dele em troca de sua integridade física. Isso faz com que sejam necessários ainda os elementos voluntariedade e consciência para

agregarem-se na figura, para que então a atitude leve o Estado ao desinteresse em proteger tal bem jurídico e, pois, afastar o caráter ilícito³⁵².

A particularidade do consentimento do ofendido, contudo, está no fato de que o consenciente deve aceitar o risco que cria e os resultados, externalizando sua disponibilidade, expressa ou tacitamente, mas a ponto de gerar no agente ofensor a certeza de que há desinteresse em proteger aquele bem, de acordo com os limites de morais e sem atingir qualquer bem jurídico de titularidade alheia ou de uma pluralidade. Há, assim, o elemento volitivo por parte daquele que dispõe do bem em questão. A partir dessas premissas, deve-se refletir sobre a conduta do usuário informático que deixa de assumir os deveres objetivos de cuidado quanto à segurança digital, conhecendo os riscos do meio e ainda assim age desidiosamente. Estaria tal cidadão consentindo tacitamente com a violação de seus bens, vez que sua ação mostra-se como um convite perceptível ao usuário mal intencionado?

Acredita-se que a resposta seja negativa, especialmente pelo fato de que deve haver uma renúncia voluntária por parte do vitimizado no que se refere ao bem, numa espécie de elemento subjetivo inequívoco, fato esse incompatível com a conduta imprudente, pois não há verdadeira intenção do prejudicado em ser vitimizado. Some-se a isso a ideia de que para que o consentimento seja válido “*deve se apresentar como um fato exteriormente reconhecível, que não admite contradições e apto a demonstrar a vontade interna*”, conforme Pierangeli³⁵³. Não se pode olvidar, também, a ideia de que, ainda que precário e desatualizado, todo o sistema informático é dotado de alguma ferramenta de segurança para evitar violações de bens jurídicos e que, havendo tais existências, torna-se contraditória a hipótese de haver o consentimento por imprudência quanto a atualizações se permanecem os mecanismos de impedimento de violações, ainda que em grau e eficácia reduzidos.

A presunção de consentimento também é ponto de importante consideração, pois que a teoria subjetiva apresentada por Pierangeli traz um interessante raciocínio que termina por descartar sua aceitabilidade no caso dos crimes informáticos. Defende o autor que tal teoria exige que, para existir a presunção de consentimento, além dos elementos do consentimento

³⁵² PIERANGELI, José Henrique. Op. cit, pp. 152-166.

³⁵³ Segundo JIMÉNEZ HUERTA, *apud* PIERANGELI, José Henrique. Consentimento do Ofendido (*na teoria do delito*). 2ª edição. Editora Revista dos Tribunais, São Paulo, 1995, p.154.

(disponibilidade do bem, consciência para dispor e voluntariedade) e da inexistência de um consentimento real, é de se raciocinar prognosticamente acerca de a probabilidade de o titular do direito consentir com a violação, se tivesse conhecimento da situação lesionadora do bem. Acredita-se, pois, que ainda que não tenha havido diligência quanto à segurança de seu dispositivo tecnológico, em estando o vitimizado presente, não haveria de aceitar que a confidencialidade, integridade ou disponibilidade de seu sistema fossem ofendidos, posto a importância de tais bens para o dia a dia³⁵⁴.

Finalmente e conforme supra, o fato de o prejudicado dever suportar a perda do direito parece não se encaixar nos crimes informáticos, pois em regra a falta do dever de cuidado leva a um arrependimento *a posteriori* por parte do vitimizado, que muitas vezes não é capaz de reverter o prejuízo experimentado, frente ao novo valor dos dados frente aos objetos materiais.

Concluimos que a atitude da vítima do delito informático poderá ser verdadeira causa excludente de ilicitude quando houver permissividade no que se refere à violação de um dos bens envolvidos com os crimes informáticos próprios ou impróprios, mas que, como regra, a prática reiterada na rede mundial de computadores leva em conta a exploração de brechas de segurança dos aparatos informáticos, mas sem que o usuário imprudente aceite o resultado lesivo ou tenha contribuído conscientemente para o acontecimento do fato. Porém, não é de se deixar de valorar tais omissões e imprudências “*in albis*”. Há a necessidade de se graduar a quantidade de contribuição dada pela vítima para medir-se corretamente a punibilidade do agente vitimizador.

AUTOCOLOCAÇÃO DA VÍTIMA EM RISCO

A lacuna deixada pela desconsideração da vítima na primeira fase da criminologia mostrou-se fundamental na inteira compreensão do fenômeno delinquente. Ao definir vitimologia, Raul Goldstein apõe que “*vitimologia é parte da criminologia que estuda a vítima não como efeito consequente da realização de uma conduta delitiva, mas como uma das*

³⁵⁴ PIERANGELI, José Henrique. Op. cit. pp. 152-166.

*causas, às vezes a principal, que influenciam na produção de um delito*³⁵⁵”.

A partir disso, há que se considerar a ideia de que em certas ocasiões é a vítima que merece atenção do operador do direito para que a culpabilidade seja atribuída ao vitimário na correta medida. Porém, a vítima que intencional e conscientemente abdica de um direito disponível seu, seja tácita, seja expressamente, recebeu consideração a partir da criação da causa supralegal de exclusão de ilicitude já enfocada, denominada consentimento do ofendido, e que traz como elementos fundamentais a liberdade para decidir sobre direitos individuais e a verdadeira disposição: há o suporte necessário da perda do valor abdicado em favor da atitude de um agente.

Há, contudo, uma lacuna que o consentimento do ofendido deixa e que gera algumas intrigas no Direito Penal, mas que o funcionalismo identifica e explora a partir das ideias de risco desenvolvidas. Tal lacuna seria aquela que se refere à situação em que há um comportamento livre e consciente da vítima e que gera resultados, não necessariamente queridos pela parte prejudicada, e não necessariamente praticados por alguém.

Dentre os principais exemplos está a situação em que dois indivíduos encontram-se se drogando e um falece de overdose. Certamente que o falecido conhecia os riscos do uso excessivo de drogas e, com sua atitude, gerou sua morte, mesmo sem ter querido atingir tal resultado. Do mesmo modo o exemplo da pessoa que, mesmo sabendo da existência de doença sexualmente transmissível no parceiro, insiste na prática de sexo inseguro. A vítima ofendida certamente não consentiu com a prática de atitudes a ela lesivas, mas conhecia os riscos e ela própria colocou-se a tomar atitudes prejudiciais a si. E é nesse contexto que a teoria da imputação objetiva tenta se adaptar.

Havendo a imputabilidade da vítima, o total conhecimento da situação de risco, a disponibilidade do bem e a colaboração total ou parcial com a criação do resultado danoso, claro está que se encontrava a vítima em estado de autocolocação em risco.

Não se está aqui apontando que a vítima quer ser prejudicada, quer que o risco gere consequências prejudiciais para si ou consinta com a violação. O que se aponta é que há uma

³⁵⁵ GOLDSTEIN, Raul. Dicionario de Derecho Penal y Criminologia *apud*. MOREIRA FILHO, Guaracy.

espécie de aceitação eventual para possíveis situações lesivas a partir da criação de um auto-risco, pois que a vítima gera para si mesma a potencialidade para tornar-se alvo de consequência danosa. Observe-se que a consequência danosa que seguirá pode ser integralmente causada pelo vitimizado ou, ainda, ser apenas facilitada pela situação de risco elevado gerado pela conduta, levando um vitimizador a completar o tipo.

O que quer o instituto da autocolocação da vítima em risco é modular corretamente o grau de culpabilidade de cada ator do fato, interpretando o Princípio da “*ultima ratio*”, da proporcionalidade e da subsidiariedade da lei penal de modo que o Estado reduza sua ação paternalista e permita que seus cidadãos acatem a existência de uma “*margem de responsabilidade com relação à proteção do bem jurídico que depende diretamente da vítima*”³⁵⁶.

Pelas ideias funcionalistas desenvolvida por Roxin, há que se pressupor a existência de riscos admissíveis na vida em sociedade e, a *contrario sensu*, riscos reprováveis, num raciocínio político criminal necessário para o estabelecimento de graus de intensidade quanto às atitudes dos indivíduos. Contudo, não restringindo seus espectros de análise, propõe o autor que o conceito de risco – criação, aumento, diminuição – também seja analisado no tipo, e inclusive pela ótica da vítima³⁵⁷. Assim, há uma expectativa social quanto ao cumprimento e acatamento dos tácitos mandamentos dos tipos penais, para que todas as pessoas ligeiramente tentadas a praticarem delitos não o façam, mas também há uma expectativa social para que todas as pessoas dotadas de meios para proteger seus bens jurídicos, o façam, deixando que o Estado preocupe-se com aqueles de mais difícil preservação.

Assim como se espera que o pretense criminoso não supere os estágios internos de cometimento de delito, também se espera que as pretensas vítimas mantenham-se em estágios ótimos de autopreservação. Não se admitiria, por tal raciocínio, nem que um vitimário criasse riscos, nem que a vítima gerasse ou aumentasse riscos, facilitando o cometimento de um delito

Vitimologia. Editora Jurídica, São Paulo, 1999, p.25.

³⁵⁶ GRECO, Alessandra Orcesi Pedro. A Autocolocação da Vítima em Risco. Editora RT, São Paulo, 2004, p. 115.

³⁵⁷ “O que ocorre de acordo com a vontade do lesionado é uma componente de sua auto-realização, que em nada interessa ao Estado (... é altamente controvertido em que medida se legitima o paternalismo estatal (...)) tal paternalismo só se justifica em casos de déficit de autonomia na pessoa do afetado (...)”. ROXIN, Claus. Estudos de Direito Penal (tradução Luis Greco). Renovar, Rio de Janeiro, 2006, pp. 44-45.

ou a violação de um bem jurídico indisponível.

Com isso, punir-se-ia com rigor o vitimário que exclusivamente cria riscos e prejudica vítimas, punir-se-ia com menor rigor aquele vitimário que pratica o crime graças à facilitação do ato delinquente por atitudes da vítima e, ainda, não se puniria o agente que não possuísse qualquer relação direta com a lesão a uma vítima. Isso porque se quer que uma vítima que age conscientemente e positivamente na criação de um risco para seus próprios bens disponíveis arque com as consequências de tal ato livre, criando-se responsabilidades.

Günther Jakobs denomina tais responsabilidades de papéis sociais. Cada vítima – pois cada cidadão o é potencialmente, com maior ou menor graduação – estaria obrigado a cumprir com seu papel preventivo pessoal, formando coletivamente um feixe preventivo. Haveria expectativas sociais para todos sob tutela jurídica, pois impossível seria a onipresença do poder central quanto a todas as atitudes de seu povo³⁵⁸.

Especificamente para os delitos informáticos, a situação mostra-se bastante semelhante. Conforme exposto, a sociedade informacional em seu aspecto informático é mera extensão “*sui generis*” da sociedade, que por sua vez constitui novo bem jurídico denominado segurança informática (ou segurança telemática), que se subdivide em aspectos privados – no caso de violações de integridade, confidencialidade ou disponibilidade que atingem exclusivamente um indivíduo – e aspectos públicos – no caso de violações que importam em prejuízo ao meio ambiente informático e que impactam em uma coletividade de pessoas.

A figura da autocolocação da vítima em risco, para o funcionalismo, adquire contorno de elemento subjetivo do tipo, ou seja, serve para dosar a quantidade de participação da vítima na conduta, podendo até mesmo chegar a afastar a tipicidade do fato.

O que releva no momento, é apresentar que a autocolocação da vítima em risco parte das premissas de que a) a vítima não age sob vícios de consentimento, tendo domínio ainda que relativo sobre a situação de risco; b) a vítima deve ser sujeito maior, capaz e competente para calcular a dimensão do risco; e c) não pode haver um terceiro em especial situação de garante quanto à pessoa que se colocou em risco.

³⁵⁸ JAKOBS, Günther. Op. cit. pp. 56-74.

A análise de tais características frente ao delito informático é importante.

Primeiramente, é de se recapitular o fato de que a rede mundial de computadores é um ambiente de riscos normais, seja pela anonimidade dos contatos, seja pela constante circulação de ameaças por códigos maliciosos. Para tanto, é indubitável que certos mecanismos de proteção são considerados mínimos para uma boa navegação. Programas de segurança, antivírus, *antispywares*, *antiadwares*, *firewalls*, senhas bem elaboradas, todas são consideradas atitudes mínimas para a evitação de violações, destruições de dados e assim por diante. Porém, ter um usuário sido relapso na instalação dos conhecidos meios mínimos de proteção, deixando de atualizar programas com *patches* de segurança, deixando de atualizar o banco de dados de *malwares* ou até mesmo instalando arquivos desconhecidos, abrindo anexos de *emails* desconhecidos, dentre diversas outras práticas, faz com que esteja o cidadão expondo-se a riscos, aumentando os riscos de violações e até mesmo deixando de proteger seu patrimônio.

O fato de a mídia propagar constantemente e os sistemas operacionais alertarem diariamente para os riscos inerentes à informática, faz com que certas medidas de segurança sejam do conhecimento pressuposto de todos os usuários interessados em conectarem-se na sociedade informacional. A inclusão digital traz consigo a cartilha de autoproteção quanto às constantes ameaças enfrentadas nos meios informáticos a ponto de tal dinamismo exigir que os próprios programas atualizem-se automática e diariamente para prevenir esquecimentos do proprietário do dispositivo. Ainda assim, por ser a informática dependente de comandos dos usuários, boa parte da cautela informática é responsabilidade do usuário.

A desobediência às recomendações de segurança dos aparatos é opção do usuário, assim como o atravessar da rua fora da faixa de segurança de pedestres é alternativa ao transeunte. Em ambos casos, o indivíduo conhece os riscos de ser vitimizado, mas ainda assim segue adiante em sua opção livremente. A primordial diferença está no fato de que, na rua, o transeunte enxerga os carros que se aproximam e pode, por suas atitudes, quiçá evitar seu atropelamento. Na rede mundial de computadores, as ameaças e ataques não raro são feitos de modo mascarado ou imperceptível. Há, pois, maior exposição aos riscos informáticos a falta do dever de cuidado objetivo da vítima quanto à administração e gerenciamento dos suportes

de segurança.

Em regra, pelo fato de ser a informática individualista, normalmente é um usuário que termina por ficar incumbido da segurança de seu bem, patrimônio, e, assim direito disponível. É critério do particular a disposição da segurança de sua máquina, podendo expô-la aos riscos que bem entender, navegar nos *sites* que achar mais adequados para suas necessidades e assim por diante. Fosse o computador de alguém destruído intencionalmente por terceiro, e criminalmente estar-se-ia diante do tipo do artigo 163 do Código Penal, ou seja, o crime de dano, que é essencialmente crime de ação penal privada. Sabidamente os crimes de ação penal privada são aqueles que exigem que o particular promova a queixa-crime para que haja legitimidade para o Estado promover o processo crime, levando-se *a fortiori* à ideia de que não tem o Poder Público, per si, o interesse em de ofício ou por meio de suas instâncias administrativas dar início a tal ação. É, assim, conclusivo o fato de que o bem, no caso, representaria direito disponível por parte de seu legitimado.

Para que os elementos da autocolocação da vítima em risco estejam presentes, não poderá haver, por parte de um terceiro, indução na criação ou aumento dos riscos (não atualização de programas, instalação de *softwares* de procedência desconhecida, etc). Terá o usuário que assumir uma atitude desidiosa quanto aos cuidados quanto a seus aparatos, consciente e livre, sem influências e persuasões.

O segundo elemento representado pela capacidade de calcular-se o risco é inerente à compreensão de que se está diante de uma sociedade eminentemente arriscada, bastando que o dispositor (ou disponente) tenha capacidade civil para ser titular do bem informático material. Porém, é notório que o conhecimento informático altera-se com certa frequência, alterado por vezes conceitos e paradigmas, gerando ao usuário a obrigação de atualização constante. Tal papel cabe em regra a revistas especializadas, suplementos especializados de jornais e até mesmo pela própria navegação diária. No caso de haver suficiente informação, Alessandra Greco aponta que:

“Não se vê nenhuma dificuldade em aceitar uma ação a próprio risco, quando a vítima foi suficientemente informada sobre o significado da conduta que realiza. O problema surge quando o

*terceiro tem maiores conhecimentos que a vítima*³⁵⁹,

No caso apontado, o fato de um terceiro ter maiores conhecimentos e isso afetar a atitude da vítima, faz com que verdadeiramente haja uma heterocolocação da vítima em risco, caso seja elementar o repasse de tal conhecimento. Caso caiba à própria vítima educar-se quanto às suas obrigações de segurança e tais informações sejam públicas, então será irrelevante a conduta do terceiro, gerando igualmente o atendimento ao segundo elemento e, pois, a autocolocação em risco.

O terceiro e último elemento trata da heterocolocação em risco por parte de um indivíduo. Caso a situação de risco tenha sido gerada por um terceiro, este assume a posição mínima de garante, conforme preceitua o artigo 13, §2º, “c” do Código Penal quando estabelece que

“Art. 13 - O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. (...)”

§ 2º - A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado. O dever de agir incumbe a quem: (...)

c) com seu comportamento anterior, criou o risco da ocorrência do resultado.(...)”

Desta maneira, caso alguém gere o risco em nome da vítima, não se pode atribuir a ela a criação da fragilidade, não se enquadrando a situação na figura. Certamente, se o terceiro for o próprio experto que na sequência violará um bem jurídico informático, nesse caso responderá ele pelo tipo, se existente.

Note-se que os crimes que admitem a ideia da autocolocação em risco são exclusivamente aqueles em que há alguma contribuição de ambos atores pois que deve haver espaço para que a conduta da vítima tenha impacto e relação com o delito. Crimes unilaterais ou violentos são cometidos sem a participação, contribuição ou auxílio significativo por parte da vítima prejudicada no que tange ao instituto em tela tendo-se em vista sempre ser caso de

³⁵⁹ GRECO, Alessandra Orcesi Pedro. Op. cit. p. 127.

criação de risco por parte do agente vimitizador.

Por óbvio, não se está defendendo, ao expor a figura da autocolocação da vítima em risco, que a vítima tem intenção de ter seu direito lesado. Em verdade, apesar da geração do risco, a vítima acredita que o desfecho quanto a seus direitos não será a ela prejudicial. Também, não se está defendendo a ideia de que a atitude da vítima justifica a conduta do vitimário e o exime de ser punido pelos atos de prejuízo que cometeu em qualquer caso. O que se quer, ao tratar deste instituto, é reduzir o estudo às hipóteses de modulação da reprovabilidade da atitude do autor nos crimes informáticos, pois que, se houve contribuição da vítima lesada quanto a seu bem particular (bem este que poderia ser espontaneamente lesado, destruído, alienado, etc), tal ação deve ter repercussão penal.

A VITIMODOGMÁTICA E SUAS IMPLICAÇÕES NA CONDUTA CRIMINOSA

Uma vez apresentada a problemática da vítima e a relevância de suas condutas no cometimento dos crimes informáticos, acredita-se necessário que se verifique como aplicar as figuras do consentimento do ofendido e da autocolocação da vítima em risco no segmento delinquencial proposto.

Desnecessário reiterar que para ambos os institutos a aplicação restringe-se a bens disponíveis, que admitem alto grau de decisão individual quanto a seu destino porquanto titularizados a particulares, tendo afastado o interesse e a pretensão do Estado em tutelá-los. Bens públicos ou que têm características coletivas não podem ser objeto de qualquer espécie de transação e sempre serão de responsabilidade da Administração Pública. Ataques informáticos a *sites* governamentais, sabotagem de acesso a provedores, disseminação pública de códigos maliciosos, dentre outras figuras que prejudicam uma coletividade serão sempre delitos de ação penal pública incondicionada e, por isso, violam necessariamente o segmento difuso da segurança informática.

A aplicação do consentimento do ofendido não traz grandes dificuldades no que se refere aos bens particulares. Isso porque caso um titular de um bem jurídico informático

(direito disponível, pois) livre e conscientemente decida por permitir que um terceiro lesione seu bem jurídico, tal atitude está dentro da esfera de ações legítimas por parte do titular do bem e isso gera um afastamento (*rectius*, exclusão) da ilicitude da conduta pois que a disposição de um direito gerando permissão de sua violação legaliza qualquer atividade praticada, pois que assentida. A permissão dada pelo titular dos dados a um técnico, para que seja feita a formatação do disco rígido, assim, é exemplo.

A autocolocação da vítima em risco, também restrita a direitos disponíveis, diferentemente do consentimento do ofendido, é uma falta de dever de cuidado objetivo, pela desídia quanto à responsabilidade que tangencia algum direito. É o desleixo de um particular, ou a ação/inação consciente, que sabidamente poderá gerar o risco de um bem jurídico sofrer um prejuízo, mas que ainda assim é cometida pela futura vítima na esperança de que nenhum mal ocorra a seus direitos. A não atualização de um antivírus na data que gera a contaminação do sistema, ou o ingresso em *sites* inseguros que prometem conteúdos falsos e que pedem a instalação de um programa espião são exemplos.

Acredita-se, pois, que no caso de haver uma análise investigativa de um prejuízo informático relatado, fundamental é que a vítima seja devidamente ouvida sobre suas atitudes antes, durante e depois dos fatos, para que seja apreciada sua contribuição no caso. Havendo criação ou aumento de risco praticado por condutas evitáveis da vítima, apesar de seu conhecimento e bom senso no sentido contrário, tal fator deve ser levado ao juízo para que este mensure a co-existência de participações dos atores do fato, estabelecendo a pena mais justa a partir de então.

UMA PROPOSTA PARA DELITOS INFORMÁTICOS

Nenhum país do mundo tem tantos habitantes quanto a Internet. A China, com seus 1,3 bilhão de habitantes não atinge população virtual, hoje com cerca de 1,5 bilhões de usuarios.

Criminologicamente, conforme interpretação da criminologia crítica, o delito deve ser estudado como um fenômeno normal na sociedade (qualquer que seja) e que deve ser mantido em níveis toleráveis, mínimos possíveis. Isso se dá porque é indissociável em uma sociedade os desvios de comportamento (*deviance*) tanto de delinquentes quanto de vítimas. De acordo

com o antiquíssimo adágio de que onde há sociedade, há direito (“*ubi societas, ibi ius*”), proporcionalmente, quanto maior for uma sociedade – e quanto mais complexa – maior a necessidade de se criar regras e traçar linhas de conduta aceitáveis.

Pois, a sociedade virtual é a maior já existente. Socraticamente, pois, necessita de direito para regrá-la a ponto de, não se trazendo normas de conduta, convívio e ação, dar-se um passo de retorno à autotutela, entretanto em uma modalidade diferente: uma autotutela em que prevalecerá o interesse dos tecnologicamente mais argutos.

Assim, a sociedade pós-industrial (ou informacional) é composta por indivíduos de classes virtuais que admitem graduação de acordo com a cultura e educação voltada para a realidade tecnológica: os que melhor dominam a linguagem e conhecem a informática, virtualmente, têm maior força no ciberespaço no que se compara àqueles que não utilizam a tecnologia exceto para finalidades mínimas de interação e trabalho.

Uma sociedade informacional sem regras levará ao prevalecimento daqueles que mais educação receberam para lidarem com o mundo dos *bits*, permitindo que sobrepujem os de menos conhecimento.

Há, certamente, necessidade de regramento transoerânico – civil inclusive – para lidar com a nova realidade. Exemplo paralelo mas de comparável e interessante aspecto são as Convenções de Varsóvia e Montreal, normativos criados e aceitos por diversas nações para o fim de lidar com o difícil problema do tráfego aéreo. Uma vez que havia problemas por conta de o transporte aéreo envolver uma grande variedade de países, convencionou-se pela unificação de regras relativas ao transporte aéreo internacional no intuito de simultaneamente assegurar proteção aos usuários de tal realidade, bem como harmonizar regras de direito no setor.

Acredita-se que o mesmo ocorre quanto ao ciberespaço. Surge a imprescindível necessidade de as soberanias unificarem-se, a exemplo da Convenção de Budapeste, buscando mínimos regramentos para lidar com as particularidades da realidade virtual que, por sua vez demanda compreensão de novas particularidades como a interatividade, a mobilidade, a conversabilidade, a conectividade, a ubiquidade, a globalização, a fracionabilidade, a divisibilidade, a intangibilidade, a disponibilidade, a pluralidade, a permissividade, a velocidade e a não territorialidade.

A partir de tais regramentos e compreensões internacionais necessárias, inicia-se a discussão sobre a criminalidade dessa nova esfera social.

Há, também, que se levar em conta que tais características tornam o ciberespaço um ambiente de liberdade extrema e baixa probabilidade de administração centralizada pelos Estados. Sua essência disseminadora de opiniões e informações faz com que seus adeptos busquem tal espaço como plataforma de ideias, desenvolvimento de produtos de informação, redes de relacionamento e comércio sem fronteiras e foco de extravasamento de preferências, desde sexuais até políticas.

Em especial a rede mundial de computadores compôs-se num ideal auto-regulamentar. Deste modo, a liberdade pregada quando da criação do ambiente virtual, tanto na navegação quanto na criação e imputação de conteúdos fez com que a Internet se fizesse um ambiente de expansão social, expansão de conhecimento e exploração de alternativas para formas de auto-desenvolvimento.

A criação de um ambiente de permissividade sem identificação levou alguns a desvirtuarem certas finalidades. A opção de utilização para fins espúrios fez com que uma parcela da sociedade virtual aproveitasse a plataforma para cometimento de atos ofensivos a valores e bens alheios. Assim, produtos como códigos maliciosos foram desenvolvidos gerando imediatamente uma conscientização quanto à periculosidade do meio virtual.

Dito isso, compreendeu-se que o ciberespaço admitia utilizações prejudiciais e, com a popularidade do meio e com a utilização massiva, tais danos mostraram-se gravíssimos.

Surgiu, então, uma nova classe de vítimas: as vítimas da virtualidade.

A evolução do estudo da vítima, por sua vez, mostrou-se deveras importante para a verificação situacional da nova vitimização. Isso porque a migração da autotutela como meio de resolução de conflitos para a jurisdição do poder central é uma realidade indissolúvel. O indivíduo lesionado, salvo raras exceções previstas, deverá reportar ao Estado sua pretensão em ver apurados os fatos que o prejudicaram.

Ocorre que o atual ambiente ciberespacial permanece um ambiente sem regramento – mormente no Brasil –, o que permite que se possa associar comparativamente com a sociedade primitiva: conhece-se os riscos, vive-se no meio por necessidade, está-se permanentemente sujeito a agressões.

Enquanto que na sociedade descentralizada primitiva de perigos o momento vitimológico era o da idade de ouro –, com permissão para que a vítima e seus próximos reagissem livremente às ofensas –, na sociedade virtual semelhante à terra sem lei e sem

soberanias, a autotutela é proibida: deve-se clamar ao Estado o apoio jurídico na persecução de delinquentes, ou seja, deverá o usuário da tecnologia submeter seu problema ao aparato estatal para trazer-lhe a solução.

Há, entretanto, problemas na habilidade das forças policiais esclarecerem os problemas surgidos no ciberespaço por faltar preparo e mão-de-obra qualificada. Há também a falta de dogmatização da nova realidade, que ainda não conta com tipos penais suficientes.

Está, pois, a vítima do fato delinquente virtual em contínuo ataque, sem respaldo legal de proteção, sem confiança nas forças de segurança e investigação e sem conseguir reagir num ambiente em que o agente criador de prejuízos sobrepuja seus alvos com sua habilidade individual, mascaradamente, sem violência e notadamente até mesmo sem a compreensão ou entendimento de sua vítima.

Isso faz com que se estabeleça um círculo vicioso, em que conhecendo tais realidades supracitadas, as vítimas cada vez menos reportem terem sido alvo das condutas violadoras de direitos e, assim, mais impunes ficam os perpetradores que, então, ficam ainda mais a vontade para permanecer no cometimento reiterado das práticas. A não denúncia dos fatos gera cifras negras altíssimas (e cifras cinzas frequentes) que naturalmente fazem com que o estudo de tal criminalidade fique aquém do ideal por falta de empirismo.

O esforço criminológico pela compreensão do tema fica adstrito a particularidades no cometimento do fato, sem as particularidades e variáveis necessárias.

O estudo da vitimologia vem em muito contribuir nessa etapa difícil. Primeiro porque ao se notar que a vítima pode ser classificada e tomada em conta a partir de conceitos como precipitação vitimal, vitimogênese, relação vítima-vitimário, auto-responsabilidade, deveres mínimos de cuidado e precaução e *iter victimae*, abre-se o leque de variáveis a serem consideradas nos estudos penais.

O fato de se examinar a delinquência a partir também daqueles que sofrem prejuízos mostra-se um pilar que compõe uma criminologia mais completa e realística pois que se conclui pela análise de delitos também sob o aspecto do relacionamento com a vítima, partindo-se do pressuposto (ou afastando-se um antigo pressuposto) de que existe uma competência da vítima, fato fundamental na compreensão da tipicidade proposta pelo funcionalismo.

Tendo-se tal ótica como imprescindível, podem os pensadores propor novos e mais

completos modelos de manutenção do fenômeno delinquente a níveis toleráveis e mínimos. Desta maneira, a proposta das teorias relativas ou utilitaristas de que a pena tem somente como foco o desincentivo e desestímulo ao criminoso frente ao delito cometido bem como à demonstração à sociedade que observa o criminoso de que qualquer um que tome a decisão de cometer um delito, fica vaga.

Diante da imaterialidade dos delitos informáticos propriamente ditos, os modelos preventivos apresentados mostram somente parcial capacidade de produzir efeitos nesta realidade. Nas palavras de Roberto Chacon de Albuquerque³⁶⁰:

“o ciberespaço também é cada vez mais a nova arena para as atividades do crime organizado transnacional, lavagem de dinheiro, crimes financeiros, terrorismo e outros crimes. Há quem diria que os criminosos têm sido muito mais rápidos em adaptar e tomar vantagem desse novo mundo e dessa tecnologia para exercerem suas atividades através dos continentes com a velocidade da luz, sem serem detectados e em segredo. A resposta dos governos e das organizações internacionais tem sido com frequência lenta, insuficiente e, na maioria das vezes, de natureza reativa”(grifo nosso)

A mera análise da problemática dos delitos informáticos seja numa perspectiva legalista, seja numa perspectiva criminológica e ainda, mais especificamente na ótica vitimológica, leva-nos a um incômodo e inquietante vazio. Certamente que há importância na identificação de problemas na nova casuística da criminalidade, mas uma proposta a partir desse estudo poderia contribuir de alguma maneira para uma melhor compreensão e manutenção de tal tendência a níveis mínimos.

Inicialmente, importante demonstrar de que modo a doutrina tem se manifestado quanto a este problema para, na sequência, apresentar-se uma proposta.

Susan W. Brenner, apresenta inicialmente quatro como as frentes de atuação para o combate ao delito informático, a que denominou nova estratégia de controle de crimes: a partir

³⁶⁰ Op. cit. Prefácio, XV.

dos apontamentos feitos pelas convenções sobre ciberdelitos do Conselho da Europa e da Organização das Nações Unidas; a partir de técnicas legais de coação pós fato; a partir de técnicas civis de reação e a partir de um aumento de fiscalização e controle nas mãos das autoridades.³⁶¹

No que se refere ao debate sobre a problemática em sentido amplo, a ONU elaborou um texto denominado “Manual para prevenção e controle de delitos relacionados com computadores”³⁶² em que aponta quais seriam os principais problemas na temática. Seriam eles:

(a) a falta de um consenso global sobre quais tipos de conduta deveriam ser considerados delitos relacionados com computadores;

(b) a ausência de um consenso acerca da definição legal de condutas criminosas;

(c) ausência de conhecimento técnico por parte da polícia, Ministério Público e das cortes ao tratar do tema;

(d) a falta de adequação dos poderes para investigar e acessar sistemas informáticos, incluindo a inaplicabilidade dos poderes de sequestro (medidas constritivas) para bens intangíveis como os dados computadorizados;

(e) a falta de harmonia entre procedimentos legais de diferentes nações concernentes à investigação de delitos relacionados com computadores;

(f) o caráter transnacional de muitos dos delitos de computador; e

(g) a falta de tratados de extradição e de assistência mútua e mecanismos de coação sincronizados que permitam a cooperação internacional, ou a incapacidade que os tratados existentes têm para lidar com as necessidades especiais de investigação de delitos de computador.

Como resposta a tais problemáticas, o Oitavo Congresso das Nações Unidas para

³⁶¹ BRENNER, Susan W. Op cit. pp. 17-22.

Prevenção de Crimes e Tratamento de Criminosos³⁶³, especificamente sugeriu como propostas:

- A) Modernização das leis e procedimentos criminais, incluindo-se medidas para:
1. Assegurar que os tipos existentes e as leis relativas a poderes de investigação e admissibilidade de evidências em procedimentos judiciais apliquem-se adequadamente e, se necessário, fazer mudanças;
 2. Na falta de leis que se apliquem adequadamente, criar tipos penais e procedimentos investigativos e para coleta de evidências que necessariamente sejam capazes de lidar com as novas e sofisticadas formas de atividade criminosa;
 3. Providenciar o confisco ou a restituição de bens adquiridos ilegalmente pelo cometimento de delitos relativos a computador.;
- B) Melhoria de segurança de computadores e medidas de prevenção, levando-se em conta problemas relacionados à proteção da privacidade, o respeito aos direitos humanos e direitos fundamentais e qualquer mecanismo regulatório pertinente a uso de computadores;
- C) Adoção de medidas para sensibilizar o público, o judiciário e as agências reguladoras sobre o problema e a importância da prevenção acerca de delitos relacionados a computadores;
- D) Adoção de medidas para treinamento adequado de juízes, oficiais e agências responsáveis pela prevenção, investigação, persecução e adjudicação de delitos econômicos e relacionados a computadores;

³⁶² Título original: “International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime”. Disponível em <http://www.sgrm.com/art26.htm> e em <http://www.uncjin.org/Documents/irpc4344.pdf>. Ambos acessos em 27.09.08 às 12:03hs.

³⁶³ As propostas constavam no documento “International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime”, disponível em <http://www.uncjin.org/Documents/irpc4344.pdf>. Acesso em 04.01.09 às 00:16hs. Boa parte das propostas foram reiteradas pelo Décimo Congresso das Nações Unidas para Prevenção de Crimes e Tratamento de Ofensores.

- E) Elaboração, em colaboração com organizações interessadas, de regras sobre ética no uso de computadores e ensinamento de tais regras como parte do currículo e treinamento em informática
- F) Adoção de políticas para as vítimas de delitos relacionados com computadores que sejam consistentes com a Declaração das Nações Unidas de Principios Básicos de Justiça para Vítimas de Crime e Abuso de Poder, incluindo a restituição de bens ilegalmente obtidos e medidas de encorajamento das vítimas a comunicarem tais crimes às autoridades competentes.

Os próprios Estados Unidos da América do Norte, nesse sentido, desenvolveram legislações e órgãos de plantão e apoio a delitos informáticos, como por exemplo o CHP³⁶⁴ (*California Highway Patrol*) e o ICCC (ou IC3 - Internet Crime Complaint Center)³⁶⁵, que tem como objetivo fornecer auxílio e presteza na investigação da criminalidade, apoiando nas investigações através da rede mundial de computadores³⁶⁶.

Quanto ao segundo ponto, o que também se questiona é qual seria o melhor método positivista de combater a criminalidade informática. E aqui se abre margem para a análise de duas possíveis ações de política criminal legalista³⁶⁷: a criação de “*do laws*” e a criação de “*do*

³⁶⁴ Site oficial da agência em <http://www.chp.ca.gov/programs/computercrime.html>. Acesso em 19.11.08 às 02:03hs.

³⁶⁵ O *Internet Crime Complaint Center* é uma parceria entre o FBI, o Centro Nacional de Crimes de Colarinho Branco e o Escritório de Assistência Judiciária e tem como missão receber, desenvolver e redirecionar reclamações referentes a crimes informáticos. Fonte: <http://www.ic3.gov/default.aspx>. Acesso em 14.12.08 às 21:38hs.

³⁶⁶ No mesmo sentido a Convenção sobre o Cibercrime (Convenção de Budapeste) que, em seu artigo 35 apõe que: “**Artigo 35º - Rede 24/7 - 1.** Cada Parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas: a) A prestação de aconselhamento técnico; b) A conservação de dados em conformidade com os artigos 29º e 30º; e c) A recolha de provas, informações de carácter jurídico e localização de suspeitos. 2. a) O ponto de contacto de uma Parte deve ter capacidade técnica para corresponder-se com o ponto de contacto de outra Parte de uma forma rápida; b) Se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de contacto assegurará que pode agir em coordenação com essa ou essas autoridades de forma rápida. 3. Cada Parte assegurará que pode dispor de pessoal formado e equipado a fim de facilitar o funcionamento da rede.” Disponível em http://ccji.pgr.mpf.gov.br/documentos/docs_documento/convencao_cibercrime.pdf. Acesso em 03.01.09 às 10:46hs.

³⁶⁷ Alguns doutrinadores já propuseram, também, sanções eletrônicas promovidas pelo poder de punir, para

not laws”.

As “*do-laws*” seriam as normas que determinam uma obrigação de fazer (ou um ônus) que, desatendida, geraria consequências. As “*do not laws*” seriam, reversamente, normas que determinam deveres de abstenção ou obrigações (*rectius*, recomendações) de não fazer.

As normas que determinam que os cidadãos sigam certa conduta são aquelas que criam sanções para o desrespeito a tal obrigação como, por exemplo, a determinação para o uso de cinto de segurança que, se descumprida, gera a sanção pecuniária. As normas que apontam para um não agir, por sua vez, pedem uma abstenção que deveria ser respeitada como o exemplo das leis penais que tipificam condutas que, uma vez cometidas, gerariam o poder-dever de punir do Estado.

Nesse propósito, leis da modalidade “*do laws*” seriam aquelas criadas para impor a alguém a obrigação de prevenir os delitos informáticos e, caso houvesse descumprimento, surgiria um ônus.

Contudo, acredita-se precipitada tal sugestão tendo-se em vista que, a partir de tal ideia, os usuarios estariam obrigados a se defenderem de ataques complexos, o que geraria um ônus deveras intenso. Para isso, estar-se-ia transferindo ao usuario a obrigação de compreender os meios técnicos de alta complexidade (programas), utilizá-los de modo adequado para impedir ações delinquentes, além de serem obrigadas a modificá-los e atualizá-los constantemente para somente assim serem capazes de afastar as ameaças de modo eficiente. Acrescente-se, ainda, o fato de que tais programas ainda deveriam ser gratuitos para garantir o acesso defensivo a todos os usuarios, o que certamente não se atine à tendência pátria. Finalmente, há a barreira da dificuldade de identificação de violação das “*do-laws*” que, como diz Jewkes:

reagir ao crime informático, a partir de disseminação de códigos maliciosos, destruição e ações para tornar indisponível o aparato, sistema ou site de um delinquente desta esfera. Contudo, deixaremos de apontar tal solução como jurídica, tendo-se em vista que os mecanismos de controle de tais atos, mão-de-obra capacitada e a provável ineficácia de tais ações além de possíveis abusos seriam problemas consequentes a serem enfrentados. Nesse sentido, REINDENBERG, J. (2004). “States and Internet enforcement”. University of Ottawa Law and Technology Journal, 1 (213) *apud* JEWKES, Yvonne. (ed) **Crime online**. Willan Publishing, Londres, 2003, p. 19.

*“Leis de prevenção ao cibercrime, em contrapartida, estariam primariamente endereçadas a condutas que ocorrem em locais privados – a casa ou escritório de alguém. Isso traria dificuldades para aqueles encarregados de fazer valer tais leis determinando seu cumprimento.”*³⁶⁸

O caráter técnico do conhecimento informático geraria uma obrigação desproporcional ao usuário e ao Estado surgiriam obrigações de punir de duvidosa aplicabilidade. Com isso, resta a criação de leis que apontam para omissões (ou não ações: *do not laws*”, entretanto, a nosso ver, mitigada pelo Princípio da responsabilidade da vítima.

Quanto à necessidade de autoridades, é imprescindível que mais delegacias de polícia estejam preparadas para atender às denúncias do cidadão atacado pelo ofensor informático; autoridade policial e judicial, devem ser capazes de compreender os novos rumos tomados pela criminalidade, os novos meios utilizados e os novos bens jurídicos. Devem ser treinadas para entender as características específicas geradas pelo novo ferramental e, então, especializarem atendimento em tais delitos.

No que se refere às reações e prevenções dos usuários, dedicar-se-á um pouco mais de linhas. Isto porque conforme bem apresenta Gulotta que não se pode deixar de buscar a melhor consciência das vítimas que favorecem as condutas criminosas porque certamente é *“mais realista tentar modificar o comportamento da vítima do que o do criminoso”*³⁶⁹

³⁶⁸“Cybercrime prevention Law, on the other hand, would primarily address conduct occurring in private places – one’s home or office. It would therefore be difficult for those charged with enforcing such laws to determine compliance” JEWKES, Yvonne. Op. cit. p. 22.

³⁶⁹ Apud ARUS, Francisco Bueno. La atención a La víctima Del delito. Actualidad Penal. Actualidad Editorial S.A. Madrid. 1990. p. 298.

Há que se recordar, também, do item 67 (a) do documento “Crimes related to computer networks – background paper for the workshop on crimes related to the computer networks” que diz que é conclusão de boa parte dos países europeus a de que “public education and awareness may reduce the number of crimes in the electronic environment. Industry – hardware and software manufacturers, service providers and others – consumer organizations and Governments may perform a common task of informing the public about the security and other risk of open electronic environments and provide them with suggestions about how to protect their interests;”. Disponível em <http://www.uncjin.org/Documents/10thcongress/10cDocumentation/10cdocumentation.html>.

A VÍTIMA NA POLÍTICA CRIMINAL DE COMBATE À DELINQUÊNCIA INFORMÁTICA

Pouco adiantaria um Estado que gaste altos volumes de recursos para retirar delinquentes da rua se seguirem havendo pessoas provocadoras de delitos, incentivadoras de condutas delinquentes alheias. É assim que a vítima pode ser vista: como uma potencial incentivadora da delinquência por falta de deveres de cuidado, falta de conscientização e até mesmo por falta de compreensão.

A somatória de uma nova sociedade alicerçada nas ideias desenvolvimentistas trazidas pela tecnologia da informação aliada com uma crescente dependência da automatização e o incremento da velocidade formaram um segmento de risco novo, bens jurídicos novos, valores individuais novos e hábitos. A vivência dentro do novo ambiente, contudo, trouxe novas obrigações, novas necessidades de cuidado e novas precauções.

Por ser um ambiente novo, difuso porque utilizado por toda a humanidade como forma de evolução e interação, a compreensão do ambiente e a devida cautela urge.

A falta de contato físico do ciberespaço, a possibilidade de se agir sem limitações e o isolamento em íntima relação com o dispositivo frio deixa o usuário em dupla vulnerabilidade: por um lado vê ambiente em que parece prevalecer a liberdade sobre o ordenamento jurídico, tentando-o ao cometimento de qualquer fato, mas por outro lado o ciberespaço deixa-o frágil e predisposto a crer nas leituras que faz e nas promessas a ele trazidas.

Tal posição peculiar e plúrima gera naturalmente necessidade de se compreender o fenômeno delinquente na rede da mesma forma, criminológica e crítica: levando-se em consideração que a vítima do delito sempre estará no ambiente em que o delito informático ocorre e também que o usuário sente tranquilidade em cometer o ato lesionador.

Daí a proposta em demonstrar que a rede mundial de computadores mostra-se um veículo primordialmente de disseminação de pornografia, de condutas apócrifas ou veladas, de geração de riquezas, de criação de famas especiais e assim por diante.

Por serem essas condutas de notório conhecimento, por ser o ciberespaço incontrovertidamente um ambiente povoado por pessoas geradoras de riscos e de atos de delinquência egoísta (ou até mesmo de satisfação em demonstrar superioridade sobre outros

usuários) que se chama a virtualidade de espaço de risco componente de uma sociedade de risco em que homens geram as incertezas e inseguranças.

Por isso, e por crer cristalino que boa parte dos delitos informáticos (puros e impuros) exigem o relacionamento entre vítima e vitimário que se objetivou a defesa de um pressuposto diferenciado no que se refere às outras criminalidades: o dever de cuidado dos usuários, propensas vítimas de ações virtuais, é diferenciado do dever de cuidado comum.

Isso se dá pelo fato de que a esfera de navegação é desconhecida em seu potencial mutável e por conta de a janela representada pela tela (do celular, do monitor, do *notebook* ou qualquer outra) exibir apenas a representação audiovisual inteligível para o usuário leigo, que em verdade não compreende a complexidade do processamento de dados³⁷⁰.

Em suma, a falta de compreensão do usuário no tocante à quantidade de processos que ocorrem veladamente enquanto de sua navegação ou uso fazem com que a grande maioria dos indivíduos que acessa o ciberespaço o faça com receio, com cautela, tendo-se em vista estar num ambiente desconhecido.

Sobre a reação dos cidadãos, em realidade se trata de uma política a ser assumida pelas vítimas atuais e futuras: a ideia de que para reagir preventivamente ao crescimento dos ciberdelitos, os cidadãos do ciberespaço serão obrigados a educarem-se e compreenderem regras especiais que vigem no segmento social virtual.

Inicialmente, deve o usuário entender que é responsável por sua própria conduta na rede mundial de computadores. Não há dúvidas de que a permissividade e a interatividade são características de todo o meio informático: para que algo ocorra no sistema ou programas de um usuário, primeiramente há a necessidade de que em algum momento tenha este dado permissão para tanto; o mesmo ocorre na virtualidade em que o uso de dispositivos gráficos e cliques de mouse ditam o destino daquele usuário.

Compreendendo o usuário sobre o fato de que é ele o responsável por seu desenvolver na rede, é imprescindível que entenda que está diante de uma sociedade especial e que riscos

³⁷⁰ Para facilitar o uso e aumentar o número de adeptos, as plataformas desenvolveram-se num padrão amigável, comercialmente interessante, e facilitador de atividades. Observe-se a evolução dos sistemas operacionais de computadores e ver-se-á que expertos queixam-se de sistemas operacionais fechados (engessados, como o Windows Vista que não permite que o usuário acesse determinados arquivos e pastas) em que não se consegue visualizar o que ocorre detalhadamente com o programa instalado no aparato.

são constantes.

O papel da doutrina, dos pensadores da informática, dos tecnólogos e dos usuarios da rede mundial de computadores, através de seus representantes é estabelecer um nível de risco tolerável no ciberespaço. Isso porque uma vez aceitos os riscos e aceita a forma como esse novo círculo social virtual existe, chegar-se-á a uma ideia acerca dos papéis de cada um dos atores da virtualidade.

Admitindo-se que duas são as classes de sujeitos da Internet, os usuarios e os criadores, é de se dizer que existem, assim, funções diferenciadas para cada um: ao criador, impera a necessidade de construir a rede do modo mais seguro possível, sem permitir que aplicativos, serviços e programas sejam meios para a ilicitude³⁷¹e/ou, uma vez ocorrendo, buscar parcerias e grupos de trabalho para evitar a propagação das ações. Em contrapartida, há que se apontar funções ou obrigações para os usuarios.

O usuario da rede não pode ser um mero espectador das ações cometidas no meio. Deve assumir responsabilidades e consequências por seus atos na superautopista, a partir da ideia de que urge a necessidade de uma descentralização do dever de cuidado. O paternalismo penal é tema que desagrada os principais pensadores, especialmente numa ciência que tem Principios que a tornam subsidiária e derradeira.

Diante disso, algumas medidas devem ser adotadas por qualquer usuario que tenha interesse em participar da comunidade virtual. É dever de qualquer indivíduo, seja na rede como em qualquer outro ambiente, que evite sua vitimização durante qualquer atividade que desenvolva. Não se pode partir do pressuposto de que o Estado punitivo é capaz de ser onipresente no mundo físico, tanto menos no mundo aparentemente infinito criado pela tecnologia da informação. Por isso, há riscos explícitos e notórios no ciberespaço e que nenhum usuario pode alegar desconhecimento.

Há verdadeira obrigação a que tome medidas de cautela como a instalação de instrumental capaz de evitar a violação a seus novos bens jurídicos (disponibilidade, integridade e confidencialidade) por dois motivos.

³⁷¹Nesse sentido, exemplificativamente, vale citar o fato de que há mais de ano a Google Inc. efetuou acordo com o Ministério Público Federal no sentido de auxiliar o combate a crimes que envolvam assuntos como preconceito

O primeiro é o fato de que, uma vez que o usuário conhece os riscos a que está sujeito e deixa de tomar as cautelas necessárias, age com despreocupação e desinteresse na defesa de seus bens jurídicos, portanto desobrigando o Estado a incomodar-se com mecanismos de proteção: não deve, assim, o Estado proteger quem não quer ser protegido, seja por manifestação expressa, seja implícita através da negligência.

Em segundo lugar, há o fato de que cada dispositivo informático mal administrado é um ferramental de alto potencial delinquente. A não prevenção quanto a seus deveres de cuidado de sua máquina pode gerar um problema de vulto maior. Uma vez que alguém permite (ou não evita) que seu sistema seja invadido, potencialmente está contribuindo para duas alternativas: a) ou o cometimento de um delito que viola exclusivamente seu bem jurídico – e arcará com seus prejuízos eventuais pelo desinteresse, conforme acima explanado; ou b) a máquina poderá ser utilizada pelo invasor como intermediária para o cometimento de outros delitos como o envio ilegal de *spams*, ataques de negação de serviço, “furtos” de identidades, número de cartões de crédito e assim por diante.

Assim, há obrigações imediatas que devem ser assumidas por qualquer usuário. O que se propõe, é que se questione sobre o quanto a inação pela desídia no dever de cuidado com um sistema pode gerar implicações para um usuário.

No ciberespaço, não há excesso de zelo.

Por isso, diz-se que cautelas como a de manutenção diária dos dispositivos conectados, instalação e atualização constante de programas antivírus, controle de acessos a *sites*, navegação prudente, instalação de programas de detecção de arquivos espões, manutenção de *firewall*, leitura de arquivos anexos de *emails* com redobrada atenção, não disponibilização de arquivos com dados confidenciais nem emprestar senhas secretas ou numerais de segurança pela rede, são ações mínimas para a navegação diária pelo ciberespaço, dentre outras.

E aqui cabe ponderação proposta por Hassemer³⁷²: até que ponto merece proteção um bem jurídico cuja tutela não interessa ao próprio titular, seja por renunciar, seja por ele mesmo colocá-lo em risco?

e pedofilia. <http://info.abril.com.br/aberto/infonews/062007/21062007-7.shl> Acesso em 29.09.08 às 02:49hs.

³⁷² HASSEMER, Winfried. Op. cit. p. 122.

Tendo-se em vista que o Direito Penal pauta-se pelo Princípio da intervenção mínima e da “*ultima ratio*” a tendência social é a de que somente haja o acionamento de tal ramo do direito público quando outros meios de solução de litígio falharem. Por esse motivo, ações como as tipificadas pela Lei 8.137/90, especialmente as que violam a ordem tributária, têm sua persecução sobrestada até o exaurimento das investigações da esfera administrativa, prevalecendo-se a intenção de arrecadação frente à punição penal.

O mesmo se diz no que se refere a delitos cometidos pela via cibernética. Diante das necessidades, diversos serviços buscaram a criação de meios de resolução de problemas por vias administrativas, como é o caso da possibilidade de banimento ou *flaming* de pessoas que participam em salas de bate papo e desrespeitam as regras; como é o caso da possibilidade de se denunciar comunidades virtuais em redes sociais que violam o ordenamento jurídico brasileiro levando ao cancelamento dessas e assim segue.

Esse movimento penal acompanha a evolução dos Estados de Direito que de assistencialistas tomam um vulto minimalista, guinando para o fim de providências públicas, para a redução de paternalismos entre outras ações.

A demonstração de que o Estado não deve ser paternalista e presente mas sim determinante de regras gerais e defensor de sua manutenção é perceptível. Mais e mais se entrega aos indivíduos a alforria da maturidade cidadã através de criação de normas básicas por parte do Legislativo e do Judiciário seguidas de um afastamento, e dando ao cidadão o livre arbítrio. Exemplo disso é a obrigatoriedade – sob pena de sanção penal inclusive – de os fornecedores informarem sobre os riscos de seus produtos como no caso do cigarro: hoje, o consumidor lê nas embalagens o risco que corre em consumindo o produto e o faz livremente, sem poder queixar-se futuramente de ter sido ludibriado.

Idem quanto às normas de elevadores no município de São Paulo, por exemplo: encontramos placas demonstrando que o passageiro deve certificar-se de que o veículo encontra-se parado no andar. Com tais precauções, a vitimização oriunda de consumo de tabaco após alerta ou oriunda de queda por falta de dever de cuidado no ingresso em elevadores terá sido cometida por atitudes da própria vítima.

O mesmo deve ser dito da recente decisão do Superior Tribunal de Justiça (Recurso Especial nº 973.725/2008) quando se posicionou acerca da desnecessidade de as empresas seguradoras pagarem o prêmio aos familiares do segurado contratante de apólice de seguro de

vida caso este tenha falecido em decorrência da ingestão de bebidas alcoólicas.

Tais exemplos apenas demonstram a preocupação do ordenamento jurídico em trazer uma nova definição de vitimologia, admitindo claramente a vitimodogmática, ou seja, o papel da vítima na gênese do problema.

As atitudes dentro do ambiente informático também seguem a tendência de criarem restrições de atuação como é o caso do recém reeditado “*Banking Code*” em que as instituições financeiras desobrigam-se a reembolsar os clientes que terminaram por serem vítimas por conta de uma negligência quanto aos deveres estabelecidos como mínimos para o uso dos serviços como cartões de crédito. Preferem as instituições educarem seus clientes e, assim, gerarem uma transferência de responsabilidade para aquele que gera a conduta prejudicial por desobedecer normas de cuidado.

A tendência pode ser seguida no Direito Penal ao buscar ampliar a tipicidade para maior justiça, inserindo em seu conceito a possibilidade de a vítima autocolocar-se em risco.

Assim, é de imperiosa necessidade para o atendimento do Princípio da individualização da pena, para o contenção social da violência em patamares mínimos e para o próprio conceito de distribuição de justiça, que se insira no raciocínio de personificação da sanção a figura da vítima.

Interessante ponto a se levar em consideração é o das cifras negras da criminalidade informática, que assumem algumas características especiais. Enquanto que se costuma dizer que as vítimas costumeiramente deixam de comunicar suas vitimizações por conta de motivos de medo, vergonha, desconfiança do sistema policial e judicial, e até por conta da vitimização secundária – advinda do sofrimento, ridicularização, estresse e perda de tempo –, é de se apresentar que vítimas de delitos informáticos por vezes sequer sabem terem sido ofendidas em seus novos bens jurídicos e, no caso de *scamming*, de *Internet banking* ou clonagem de cartões, chegam até a serem desestimuladas a reportar o acontecido. Esse estímulo à cifra negra que envolve delitos direta ou indiretamente relacionados com instituições bancárias se dá pelo fato de que a imagem e a credibilidade dos serviços *online* podem ser comprometidos e gerarem prejuízos econômicos por uma menor adesão à virtualidade e um retorno aos custosos serviços *in loco*.

Some-se à cifra negra apontada o conceito de cifra cinza (*chifre grief*) em que o delito informático chega a ser denunciado porém jamais se atinge seu esclarecimento porquanto a

vítima desconhece seu vitimário e também porque raras são as delegacias de polícia especializadas na persecução de tais delitos mormente pela dificuldade de se obter informações de provedores de serviços – também por lacunosa legislação determinante de obrigações de tais fornecedores³⁷³ – e profissionais qualificados para realização de perícias digitais, levando ao total desconhecimento da autoria e materialidade, numa denúncia inócua³⁷⁴.

Para tanto, é imperioso que programas de política criminal sejam estabelecidos levando-se em consideração tais particularidades. O funcionalismo penal, do modo como desenvolvido por seus expoentes, procurou levar em consideração determinados vieses de difícil explicação pelas antigas teorias, tornando a tipicidade penal mais complexa.

Assim, não seria de tudo errado considerar que assim como houve um foco no desvalor do resultado que em seguida teve o acréscimo da importância do desvalor da ação, é possível falar de um verdadeiro desvalor da conduta vitimal.

A reprovabilidade da conduta de uma vítima mostra-se capaz de influenciar sobremaneira diversos delitos, em especial aqueles que envolvem relação (*rectius*, interação) dos sujeitos envolvidos.

Há que se apontar que a vitimodogmática, no que se refere ao papel da vítima na conduta delituosa, abarca diferentes correntes, de tal sorte que (i) uma delas defende uma redução na pena do autor em razão do “comportamento participativo” da vítima, considerando exclusivamente o âmbito de fixação judicial da pena – defendida por Hassemer e Gunther e (ii) outra que entende mais correto haver total isenção da responsabilidade também em razão do comportamento da vítima – defendida por Schunemann³⁷⁵.

³⁷³ Em sentido oposto, Estado de São Paulo promulgou a lei 12.228 de 11 de janeiro de 2006 que *Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providência, regulamentada pelo Decreto nº 50.658 de 30 de março de 2006.*

³⁷⁴ Mesmo nos casos de países em que existem leis que tipificam cibercrimes, ainda assim as cifras negra e cinza são altíssimas. De acordo com Yvonne Jewkes, apenas 10% dos crimes relacionados com informática são denunciados, dos quais somente 2% atingem estado de processo-crime. DOT.CONNS, Willan Publishing.p. 16, 2002. Também nesse sentido, ROMERO COLOMA, Aurelia Maria. Las Relaciones entre La Victima y su Agressor. Actualidad Penal. Actualidad Editorial, S.A., Madrid, pp. 177-185.

³⁷⁵ SILVA SANCHEZ, Jesús María. La víctima-dogmática em El derecho español. *Victimología : VIII Cursos de Verano en San Sebastián = VIII Udako Ikastaroak Donostian / Antonio Beristain Ipiña (dir.), José Luis de la Cuesta Arzamendi (dir.)*, San Sebastian, 1990, p. 197 *apud* LUCAS, Ana Cláudia Vinholes Siqueira de. Vitimologia e Vitimodogmática: uma abordagem “garantista”. In *Revista Transdisciplinar de Ciências*

A escolha (ou omissão) do usuário pela opção do programa a ser utilizado para navegação, a aceitação na instalação de aplicativos acessórios, atualização do antivírus, e assim por diante, são decisões fundamentais para a vitimização. É o meio informático eminentemente interacional e as ações tomadas repercutem, por vezes, nas consequências delinquentes permitindo a modulação da reprovabilidade.

As vítimas surgidas na nova sociedade necessariamente são avaliadas a partir do novo bem jurídico, frente a seus interesses e atitudes. Os órgãos públicos e privados, notando a progressão científica e o dinamismo com qualidade, adaptaram-se à nova tecnologia, gerando serviços ao público através da informática. Do mesmo modo, particulares passaram a gerenciar suas vidas e atividades (desde bancárias até de lazer) a partir da informática, gerando uma espécie de dependência. Os *bits*, combinados e formando informações, ganharam status de valiosos e a nova sociedade passou a explorar esse novo segmento. Imediatamente, surgiu a delinquência.

Como toda delinquência, seu desenvolvimento ocorreu empiricamente, por tentativa e erro, e através de interações experimentais para melhor desenvolvimento de técnicas que gerem mais sucesso na empreitada ilegal. Como os novos bens jurídicos limitaram-se às minúcias da segurança informática (confidencialidade, integridade e disponibilidade), as informações mais preciosas guardavam relação com violações de tais meandros.

A partir da criação de padrões de violação do novo bem jurídico, e por conta de a repetição e a constância serem características fundamentais para a criação de um tipo penal (tipicidade material), além da reprovabilidade, com a geração de prejuízos, diversos Estados decidiram por tipificar condutas informáticas como delitos. Muitas tipificações levaram em conta novas ferramentas para o cometimento de antigos tipos, numa roupagem tecnológica. Outras, geraram punição para condutas novas que violavam novos valores.

Porém, o que se nota é que o crescimento da criminalidade informática permanece. Por isso, somente o estudo completo dos delitos mostra-se realmente eficaz para a criação de políticas criminais de contenção do novo ramo delinquential. Nota-se que a análise dos delitos mais comuns revela um viés em que o comportamento da vítima é determinante para o sucesso

ou não do vitimizador. Nota-se, também, que há usuarios informáticos diferentes, que devem ser observados de forma diferente pois que certos delitos exploram falhas ímpares de certas classes.

Finalmente, a batalha pela análise do delito em todos os seus ângulos pede que se saiba como lidar com a conclusão: a vítima tem bastante relação com o cometimento do delito informático que sofre. E a análise dos institutos do consentimento do ofendido e da autocolocação da vítima em risco mostram-se importantes, pois apresentam soluções dogmáticas para a participação do vitimizado.

O consentimento, causa supralegal de exclusão de ilicitude, apresenta pouca inovação porquanto pressupõe a aceitação de lesão por parte de um usuario, fato que torna a conduta não reprovável por não haver sequer relevância penal aos olhos do Estado.

A autocolocação da vitima em risco, por sua vez, nasceu como interpretação alemã para auxílio na construção da ideia de criação de riscos na análise subjetiva do tipo, desenvolvida inicialmente por Roxin. A interpretação vitimológica do tipo também ganha relevância, gerando a ideia de que cada vítima deve assumir o grau de responsabilidade para a preservação e segurança de seus bens particulares e, pois, disponíveis.

Com isso, conclui-se que o Estado é incapaz de controlar também as relações particulares, que envolvem bens particulares – disponíveis – em nível penal. Para isso, é de se compreender a aceitação de um Principio vitimológico que anui com a ideia de que cada pessoa deve assumir responsabilidade e dever de cuidado por aqueles bens jurídicos de interesse exclusivo. Com isso, ficaria o Direito Penal mais próximo de cumprir em seu papel ideológico de ser subsidiário a todas as outras esferas jurídicas e sociais, somente como última razão, cabendo a primeira razão (raciocínio) partir de cada usuario da rede mundial de computadores para sua própria preservação.

Propõe-se que com o enraizamento da cultura da rede na sociedade, os usuarios passem a ter um verdadeiro dever de agir no momento em que se conectam à rede.

Não há dúvida de que o resultado da lesão ao bem jurídico através da forma eletrônica, em alguns casos, deve-se a própria vítima, que lhe deu causa. É perceptível que diversas

condutas vitimais, em delitos de relacionamento (ação) e até mesmo em delitos unilaterais (omissão), são fundamentais para que o resultado ocorra (art. 13 do Código Penal). O que resta saber é até que ponto pode-se atribuir à falta de precaução de uma vítima uma consequência³⁷⁶. A questão seria, então: até que ponto uma omissão informática pode ser irresponsável. A criação de Principio vitimológico de autoresponsabilidade da vítima são uma forma de reduzir-se a desproporcionalidade da aplicação da lei penal, criando obrigações e mantendo a ideal subsidiariedade da ciência penal.

³⁷⁶ No mesmo sentido HASSEMER, Winfried. Op. cit. p. 122.

CONCLUSÃO

1. A informática trouxe novos paradigmas para o pensamento penal, por conta de trazer consigo características que exigem que valores clássicos como a pessoalidade da relação criminosa, a teoria da atividade na consideração do local do crime, a limitação física do cometimento do delito, o cometimento individual de delitos, entre outros devam ser refletidos novamente, sob um novo véu. Desse modo, as características trazidas pela tecnologia refletem sobremaneira no modo como o Direito Penal deve adequar-se e interpretar seus valores.
2. A própria rede mundial de computadores é *per si* um ambiente de risco, vez que permeada pela anonimidade dos usuarios e pelo alto grau de êxito, o que estimula e multiplica a oportunidade de cometimento de delitos, sob uma máscara aparente de impunidade. Por isso e pela importância que tomou frente à sociedade, pode-se considerar a Internet como um verdadeiro meio ambiente pois que fundamental para o desenvolvimento e clamante de proteção.
3. A intangibilidade do meio, o perfil do delinquente informático e os novos bens jurídicos com necessidade de proteção fazem com que os conceitos de prevenção primária, secundária e terciária exijam nova reflexão. Os métodos antigos de prevenção têm se mostrado ineficientes pois o delinquente informático em nada se assemelha ao comum e, por isso, requer cuidados diferenciados do Estado para que não haja nova vitimização.
4. O novo bem jurídico urgido pela informática é a segurança telemática e isso se dá pelo fato de que a tecnologia formada por *bits* mostra-se melhor um meio ambiente do que um objeto individualizável. Destarte, assim como outros meios ambientes, exige-se concepções novas de bem jurídico imaterial que apontam para valores como a) a confidencialidade dos dados produzidos e armazenados pela informática; b) a integridade de tais dados; e c) a disponibilidade de acesso, leitura e uso de tais dados
5. Os novos valores ora são individualizáveis, ora são coletivos. Quando dizem respeito a um usuario em particular, por lidarem com elementos de segurança informática exclusivos,

está-se diante de bem jurídico particular e plenamente disponível, que somente será perseguido pelo Poder Público se interessar ao usuário. Quando dizem respeito a ambientes que interessam a uma coletividade, à própria estrutura da rede, ou violam bens jurídicos determinados pelo Estado como de relevância pública – segurança, vida, infância e juventude, etc –, então são indisponíveis e exigem instauração de ação penal pública incondicionada.

6. A legislação internacional não é uníssona na tipificação dos crimes informáticos nem na forma de cooperação e combate a tais delitos. O combate individual das soberanias mostra-se ineficiente, tendo-se em vista a velocidade, a mundialização e a ubiquidade serem características dessa nova delinquência e gerarem dificuldade de persecução criminal profícua por limitações inter-soberânicas e dificuldade em composição de indícios de autoria e materialidade, também por haver prejuízo na efetivação de mecanismos de constrição.
7. Outro fator que atrasa o combate da nova criminalidade é a baixa comunicação dos delitos por parte das vítimas que ou temem nova vitimização policial (secundária) ou envergonham-se de terem sofrido ataques informáticos, ou, ainda, sequer percebem terem sido vitimizadas por conta de o meio informático mascarar os danos por sua imaterialidade.
8. A ação dos delinquentes informáticos presume certo perfil. Essa criminalidade se mostra cometida por um grupo restrito de pessoas, predominantemente do sexo masculino, de razoável cultura, razoável status social e acesso à tecnologia. Em regra, os ataques informáticos exploram as características do novo meio ambiente e as fraquezas das vítimas, o que faz com que o autor do novel delito seja criativo e perspicaz na escolha e na estratégia de abordagem dos usuários que almeja vitimizar.
9. Diversas são as teorias de vitimização. Em todas, a busca é por raciocínios que encontrem uma lógica de receptividade ou potencialidade vitimal. Isso porque é pacífico o fato de que a nova criminologia compreende a vítima com papel fulcral no entendimento do delito, sendo verdadeiro ator do fato delitual, interagindo e por vezes contribuindo para o cometimento do delito.
10. Há carência e grande dificuldade de se obter padrões internacionais para o combate da

delinquencia informática na rede mundial de computadores, fazendo com que os esforços para proteger os cidadãos que convivem no meio virtual obtenham baixa proficuidade. Os recursos públicos são limitados, pouco sofisticados frente aos recursos dos delinquentes e a legislação é comumente atrasada.

11. O reconhecimento da ampla debilidade dos Estados em combater a nova tendência da criminalidade leva à busca por alternativas de manutenção da delinquência a níveis normais. Para tanto, a criminologia busca compreender os delitos informáticos em espécie, no afã de elaborar propostas de política criminal de melhor eficiência. Tendo-se em vista que a ponta repressiva mostra-se aquém das expectativas, os esforços voltam-se para a ponta preventiva da relação criminal. Para que a prevenção se mostre eficiente, é imprescindível que os axiomas de prevenção do mundo material sejam rediscutidos com vista às novas particularidades do meio.
12. A rede mundial de computadores mostra-se um cenário em que os usuarios, potenciais vítimas, são, em diversos casos, os condutores de seu próprio rumo e destino virtuais. Por isso, devem importar-se em compreender o meio em que navegam para evitar condutas que impliquem numa gratuita autocolocação em risco, apreendendo as principais modalidades de delinquência a que estão expostos e as formas de evitação, bem como os perfis buscados pelos vitimários e as fragilidades que são exploradas.
13. A vitimodogmática mostra-se como o estudo do comportamento da vítima na gênese do delito, partindo de raciocínios como o de concorrência de culpa, co-responsabilidade e perquirindo a existência de um Princípio Vitimológico que propugna a ideia de que todo cidadão tem parcela de responsabilidade pela evitação de sua vitimização, responsabilizando-se por suas omissões e negligências nos cenários em que há possibilidades de prevenir o acontecimento de delitos.
14. Enquanto que *firewalls*, antivírus, e outras barreiras existem, a efetividade de tais precauções depende da forma como o usuario as emprega. A mera crença na eficácia das ferramentas de proteção do ambiente virtual não é suficiente para a segurança do meio; apesar da sensação de segurança proporcionada pela tecnologia, cada usuario deve entender-se como um administrador de seus próprios bens jurídicos virtuais em alguma

medida.

15. A vítima, então, mostra-se capaz de contribuir para o controle da delinquência imaterial que está potencialmente presente em todos os lugares simultaneamente, fato impossível ao poder central. A prevenção primária que se mostra útil a longo prazo para evitar que cidadãos cometam delitos comuns acaba por mostrar-se especialmente eficiente considerando-se as potenciais vítimas de delitos e não os delinquentes.
16. A vitimodogmática propõe que de acordo com a forma de comportamento da vítima, haja um melhor equilíbrio na equação da apreciação de culpabilidade e dosimetria de pena. A apreciação das condutas dos usuarios vitimizados deve ter larga relevância e a análise *ex post* deve levar em consideração a capacidade de cada usuario lesionado frente ao ato sofrido. Essa ponderação pode levar, em níveis extremos, a atipicidade da conduta e, em níveis moderados, à redução da puibilidade do agente proporcionalmente.

Adware: São aplicativos em que faixas de anúncio são exibidas enquanto o programa está sendo executado. Geralmente contém códigos que permitem que dados do usuário sejam capturados e enviados para o anunciante ou fornecedor do programa;

Antivírus: Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso;

Assinatura digital: Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser;

Ataque: Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço;

Autoridade certificadora: Entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc;

Autenticação: Medida de segurança em que o acesso à rede ou a programa exige que o usuário digite um nome de usuário e uma senha de segurança e que, assim, identifica-se o indivíduo antes que ele possa acessar quaisquer dados;

Backdoor: Uma entrada secreta para acessar um sistema informático ou programa geralmente instalado por um usuário que intenta ingressar sem ser percebido;

Banda Larga: Conexão rápida em que a transmissão de dados se faz através da conexão de cabos e permite ganho em velocidade se comparado à conexão discada;

Banner: propaganda online feita por faixas e que ligam o usuário a páginas dos anunciantes através de clique;

Binário: qualquer arquivo que contém linguagem não decifrável pelo ser humano e que pode ser transferido por tecnologia informática, composto por números 0 e 1 que representam a passagem de energia (1) ou a não (0) e que são interpretados por dispositivos informáticos em grande velocidade;

Biometria: A ciência que se utiliza de propriedades biológicas como impressões digitais, marcas da retina, voz, pele, entre outros para identificar indivíduos;

Blog: é um *site* ou seção de um *site* em que usuários podem inserir informações cronologicamente, seja na forma de pensamentos, seja na forma de *links* ou imagens e

³⁷⁷ Elaborado com o cruzamento e tradução das informações de “NETLINGO – THE INTERNET DICTIONARY” (disponível em www.netlingo.com) e a Cartilha de Segurança para Internet v.3.1 do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – CERT.BR (disponível em <http://cartilha.cert.br/>)

compartilhar com outros usuarios. É uma espécie de fórum aberto de postagem de comentários e informações, em forma de diário;

Bluetooth: É uma tecnologia específica para ligações de dispositivos por meio de ondas de radio de curto alcance, que dispensa, assim, o uso de cabos e que serve para a troca de arquivos;

Bot: Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc;

Botnets: Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc;

Browser: É um programa utilizado para ver, baixar, carregar, navegar por e acessar documentos na Internet. Também conhecidos como navegadores, os principais são o Internet Explorer, o Firefox, o Eudora e recentemente o Chrome;

Bug: é um erro de programação que faz com que aplicativos e sistemas informáticos comportem-se de modo anômalo, produzindo resultados incorretos e/ou gerando falhas de performance;

Byte: é a unidade fundamental de dados para computadores e dispositivos informáticos representado por 8 *bits*. É também a unidade padrão de medição de arquivos armazenados;

Carnivore: Ferramenta de vigilância de *emails* desenvolvida pelo FBI, capaz de monitorar, filtrar e detectar palavras selecionadas, identificando os interlocutores e informando as agências de segurança para tomar eventuais providências;

Certificado digital: Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade;

Chat: Uma forma de comunicação interativa online em que usuarios podem comunicar-se com outros usuario conectados, em tempo real, a um *site*. Geralmente se classificam de acordo com o assunto tratado e podem ou não exigir autenticação para os usuarios;

Checkbox: Uma caixa de diálogo (pequeno quadrado) em que um usuario pode clicar interagindo com a página da rede e que, em clicando, faz com que uma marca apareça ou desapareça gerando consequências no preenchimento de formulários ou na contratação de serviços;

Chip: redução da palavra microchip, é um modulo complexo de circuitos muito diminutos com alta capacidade de processamento de dados;

Click: é a onomatopoeia do sim gerado quando se pressiona os botões do mouse, significando, pois, a ação de selecionar ou ativar algo através desse procedimento, no ambiente virtual;

Clique Aqui: frase comum na Internet, em especial na interface gráfica “www” usada para encorajar o usuário a clicar em um botão, *link* ou qualquer outro gráfico e, assim, ser levado a outra página;

Conexão segura: Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH;

CPU: sigla que representa a expressão “Central Processing Unit” ou Unidade de Processamento Central, é, em realidade o microprocessador responsável pela administração e tratamento dos dados;

Crack: Como verbo, significa o ato de invadir ou quebrar códigos, acessos ou dispositivos de segurança de programas. Como substantivo, representa o programa capaz de efetuar a quebra explanaada automaticamente, sem necessidade de intervenções do usuário;

Cracker: é o jargão *hacker* que descreve alguém que quebra a segurança de um programa ou sistema;

Criptografia: é a ciência de codificação de mensagens, através de sistemas matemáticos, para que não possa ser lida por qualquer pessoa, exceto o destinatário dela;

Customizar: vem da palavra inglesa “custom” que significa de acordo com as particularidades e *hábitos* pessoais. Assim, o verbo customizar significa fazer mudanças em um programa, num sistema ou até mesmo na rede para que esta fique de acordo com as necessidades pessoais de cada usuário. De uma certa forma, é um modo de personalizar o ambiente informático como melhor agrada ao usuário;

Ciberataque: É uma forma de ameaça no ambiente virtual em que o vitimizador visa atacar empresas ou agência governamentais para obter informação sensível e confidencial, geralmente com valor para venda ou troca;

Ciberbullying: é o ataque com fins de amedrontamento feito através da Internet, por telefone celular ou outro meio informático, geralmente contra crianças ou adolescentes, com intuito de humilhar, constranger, atormentar ou assediar simplesmente pelo prazer de rebaixar outro usuário, numa demonstração de superioridade e controle por parte de outra criança ou adolescente;

Cibercafe: Estabelecimento público, existente no mundo real, em que pessoas podem comer e beber e que também oferece serviços de acesso à rede mundial de computadores e a jogos;

Ciberpolicial (ou cibercop): É um investigador especialista em ações informáticas, capaz de analisar os dados existentes na rede para detectar e tomar providência quanto a delitos como fraudes, assédios, e abusos;

Ciberfraude: refere-se a qualquer tipo de enganação feita através de condutas desleais, injustas ou ilegais que ocorrem online, exemplificativamente intrusões informáticas, “furto” de identidade e condutas que envolvem cartões de crédito;

Cibernético: É o estudo que envolve diversas áreas de conhecimento conjugadas, incluindo o estudo dos seres vivos e sua conjugação com outras ciências como a computação, o processamento de dados, a filosofia social, a epistemologia, entre outras;

Cibersexo: refere-se à noção de relação sexual online ou de sexualidade virtual em que há simulação, estimulação ou interação comunicativa com objetivo de satisfazer a lascívia;

Ciberespaço: refere-se ao mundo virtual, online, imaterial que existe lastreado em sua estrutura física mas que gera uma realidade paralela e uma sociedade parcialmente autônoma;

Ciberstalker: é o usuário obsessivo, que persegue e persiste em comunicar-se com alguém pela informática, gerando medo e apreensão por conta da violência do assédio que perdura por longo tempo;

Ciberterrorismo: Termo que designa atitudes criminosas cometidas por usuários mal intencionados no intuito de destruir computadores, sistemas e derrubar sistemas de telecomunicação, com finalidades políticas, fundamentalistas ou meramente por diversão ou prejuízo alheio;

Ciberturista: Gíria para aquelas pessoas que só acessam a Internet em finais de semana ou feriados;

Decodificação: é a conversão de arquivos codificados para sua forma original permitindo que o usuário compreenda a informação ali constante;

Deletar: remover um arquivo ou apagar uma informação;

Desktop: área de trabalho de um sistema operacional;

Dial-up: é o modo discado de acesso à Internet utilizando-se de um modem conectado à linha telefônica;

Dotcom: é o sufixo “ponto-com” que designa uma atividade comercial por parte de um *site*;

DoS: abreviação de Denial of Service ou negação de serviço, é o resultado de um ataque múltiplo a um mesmo alvo (que pode ser um *site* ou um email) que, sobrecarregado, passa a responder de modo negativo às solicitações de acesso;

Download: é a transferência de arquivo de um dispositivo informático para outro;

E-bomb: é a gíria utilizada para designar um vírus muito poderoso e capaz de gerar danos a arquivos;

E-business: qualquer negócio que se perfeça a partir de um meio eletrônico, usualmente a Internet;

E-commerce: significa a condução de um negócio através de mecanismos eletrônicos, seja por conexão, seja por manutenção de *site* para divulgar, ofertar ou até mesmo vender produtos ou serviços;

E-mail: também denominado correio eletrônico, é o meio através do qual se envia e recebe mensagens instantaneamente, sem restrições de tamanho ou anexos;

Encriptação: é o processo de proteção de informação sensível durante o percurso de envio de um dispositivo informático para outro, transformando a mensagem ou arquivo em linguagem codificada, sendo somente decifrada pelo destinatário, preservando-se, assim a confidencialidade;

Endereço IP: Este endereço é um número único para cada computador conectado à Internet, composto por uma sequência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25;

Engenharia social: Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações;

Falsa identidade: Ato onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras;

Firewall: é o programa ou o sistema através do qual se cria uma barreira protetiva contra acessos não autorizados monitorando o tráfego de dados e segurando as portas através da qual um ataque poderia ocorrer;

Flame (flaming): é o ato de enviar mensagens insultantes para alguém por *email*, SMS, bate-papo e até mesmo em fóruns de discussão e que causa constrangimento;

Gamer: é a pessoa entusiasta que utilize a Internet ou quaisquer dispositivos eletrônicos com o intuito de jogar jogos;

Geek: é o termo popular que designa aquela pessoa que tem grande conhecimento de computadores, informática e Internet;

Hacker: é um entusiasta da computação que dedica-se ao aprendizado do sistema informático, da programação, do funcionamento da máquinas e seus segredos, elevando os sistemas ao maior nível de capacidade;

Hard Drive (HD): meio de armazenamento de arquivos de dados eletrônicos através de meios magnéticos, químicos, físicos ou outros meios e que serve como a memória principal de estocagem de informações;

Hardware: são os componentes eletrônicos físicos que fazem com que a seja possível o processamento de dados como, por exemplo, as placas, as memórias, o monitor, etc.).

Host: é um computador que funciona como ponto de partida e de fim da transferência de dados, também conhecido como o local onde ficam hospedados os *sites* e os provedores;

Honey pot: é uma isca que serve para atrair e prender usuários mal intencionados;

Infravermelho: uma espécie de ondas invisíveis com comprimento de onda abaixo da do espectro vermelho e que pode ser usado para transmitir dados;

Interativo: é a capacidade dinâmica de usuarios manipularem aplicativos, interagindo com o desenvolvimento dos eventos ocorridos nas plataformas informáticas;

Interface: é a porção do programa que interage entre o usuario e as funcionalidades dos aplicativos;

Intranet: é uma rede privada dentro de uma companhia ou organização que serve para compartilhamento de arquivos e programas, e que é destinada a uso de pessoal interno somente;

Invasão: Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador;

Invasor: Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão;

IP: é o endereço numérico dado a cada servidor e usuario que se conecta à Internet e que a ele ficam atrelados os registros de navegação, além dos dados pessoais da conta utilizada para obter o acesso, permitindo o rastreamento;

Update: é uma atualização de um programa ou sistema, geralmente com intuito de corrigir falhas de segurança ou aumentar suas funcionalidade. **Keylogger:** é um programa de computador ou um aparato designado para gravar as teclas que um usuario digita em um período de tempo, remetendo tais registros para alguém que, com base nisto, consegue descobrir senhas e outras informações;

LAN: abreviatura de “*Local Area Network*” ou “rede local”, que designa a interconexão de um número pequenos de máquinas entre si, através de linhas telefônicas ou até mesmo cabos, com finalidade específica;

Laptop: computador portátil, leve e que pode ser utilizado no colo, também conhecido como notebook;

Link: é o texto ou a imagem existente na rede mundial de computadores que, pela interface gráfica, permite que o usuario clique nele, com o intuito de obter acesso a algum outro documento, navegar por outros locais do ciberespaço e até mesmo interagir com o *site*. Também são chamados de “*hyperlinks*”;

Log: é um arquivo que fica guardado na máquina com o registro das atividades ocorridas durante a navegação na rede ou no servidor;

Login: é o ato de conectar-se ou acessar um computador, sistema, rede ou *site*;

Logoff: é o ato de desconectar-se de uma rede, sistema remoto ou *site*;

Mailbox: é o diretório em que os dispositivos informáticos armazenam as mensagens de *email*;

Malware: abreviação de “*malicious software*” ou “programa malicioso”, é o termo que representa códigos criados com intenções espúrias e/ou lesionadoras de arquivos e sistemas alheios;

Matrix: termo cunhado por William Gibson na novela *Neuromancer*, refere-se à rede mundial de computadores;

Dispositivo móvel: é qualquer aparato informático capaz de ser movimentado e transportado sem perder suas funcionalidades como, por exemplo, notebooks, telefones celulares, etc;

Modem: é a sigla que significa Modulador-Demodulador e representa o aparelho conectado simultaneamente a um dispositivo informático e à linha telefônica e traduz os dados para que haja interação, comunicação e envio de dados a partir dessa tecnologia.

Mouse: é o dispositivo informático que, conectado ao computador, serve para controlar o cursor da tela e que contém botões que, clicados, acionam o local da tela em que a ponta do cursores se encontra, gerando atitudes como mudanças de página, downloads de arquivos, etc;

Navegar: é o ato de movimentar-se através da rede mundial de computadores, através de links clicáveis, mudando de páginas e servidores;

Newbie: é um novato, recém ingresso na Internet ou leigo em informática em geral;

Offline: é o estado em que um dispositivo não se encontra conectado a um sistema ou rede mundial de computadores;

On-demand: refere-se a serviços oferecidos de acordo com a demanda do cliente, que o solicita de acordo com sua necessidade consumista;

Online: é o estado em que uma máquina está ligada à rede, a um programa ou a um serviço, podendo, assim interagir e comunicar-se reciprocamente.

Online Banking: é o serviço bancário fornecido através do *site* do banco, e que pode ser utilizado pelos usuários quando estão conectados na Internet

Open Source: significando fonte aberta, representa o tipo de programa que permite que os usuários tenham acesso a linguagem utilizada para sua criação, permitindo inclusive modificações por desenvolvedores e análise por expertos.

Opt-in: é o ato de um usuário explicitamente requerer o recebimento de mensagens de determinado remetente.

Opt-out: é o ato de um usuário determinar a cessação de envio de mensagens de determinado requerente.

Pacote: é o nome dado à unidade de dados enviada através da rede, por meio de sua linguagem própria.

Palmtop: é um dispositivo informático que cabe sobre a palma da mão (por isso o nome composto pelas palavras palm: palma e top: sobre), que contém sistema operacional e diversos recursos.

Password: tradução de “palavra para passagem”, também conhecido como passcode (“código para passagem”), representa os sinais co-relacionados com o nome do usuário, utilizados ambos para autenticar e permitir acesso a sistemas ou programas.

Phishing: Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Pirataria: é a atitude de copiar arquivos e programas protegidos por direitos autorais, sem licença ou autorização.

Plataforma: o tipo de sistema operacional no qual os aplicativos de um computador funcionam

Podcast: uma espécie de arquivo de áudio geralmente gratuito e que pode ser ouvido nos mais variados dispositivos multimídia.

Pop-up: expressão que significa a ação de aparecer uma tela repentinamente na tela do computador.

Post: é um substantivo que significa postar, ou seja, colocar em algum local. É jargão de informática que significa a colocação de arquivos ou informações em um *site*.

Preferências: são a personalização dos aplicativos do dispositivo eletrônico que fazem com que fique mais próximos das necessidades práticas ou até mesmo estéticas do usuário.

Programa: outro termo para *software*, é basicamente uma lista de instruções escritas em linguagem de programação e que dizem ao dispositivo como executar certas funções e cumprir com tarefas de modo específico.

Protocolo: é uma especificação que descreve como os dispositivos informáticos comunicam-se com a rede mundial de computadores ou outra rede.

Proxy: Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Remoto: controlado à distância.

Rootkit: Conjunto de programas que tem como finalidade esconder e assegurar a presença de

um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

Scam: Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan: Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*.

Screenlogger: Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição onde o *mouse* é clicado. Veja também *Keylogger*.

Shareware: é uma espécie de programa disponível na rede mundial de computadores que pode ser baixado por usuarios e que permite o uso livre de tarifas, por um período de tempo, para que o usuario possa testá-lo. Após o periodo de tempo, a funcionalidade do program cessa ou diminui, e somente após a aquisição da licença permite o retorno à funcionalidade total.

Site: é o sítio, um local virtual na rede mundial de computadores, com características audiovisuais e em que se hospedam informações que podem ser acessadas por usuarios que com ela interagem.

SMS: Do Inglês *Short Message Service*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

Sniffer: Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuarios), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Rede social: é um *site* central, uma espécie de plataforma, que agrupa e centraliza *sites* particulares feitos por usuarios, permitindo a socialização de pessoas a partir de interesses comuns.

Spam: apelido dado às mensagens comerciais não solicitadas que podem ou não ser enviadas sem o consentimento do destinatário.

Spyware: é um programa capaz de capturar informações sobre um usuario conforme este navega pela rede mundial de computadores, assim descobrindo *hábitos* e criando perfis, violando, pois a privacidade.

Sincronização: é a ação de copiar arquivos de um aparato para outro e vice versa, atualizando-os reciprocamente quanto às informações contidas no outro dispositivo.

Sistema: é a instalação completa de um computador, incluindo os programas necessarios para o funcionamento e seus periféricos, todos integrados.

Telemática: é a ciência que combina telecomunicações e informática.

Trojan Horse: é uma forma de vírus disfarçado de programa inofensivo.

Upgrade: modificar um sistema ou um programa para uma versão mais nova.

Upload: copiar um arquivo a partir de um computador para um servidor ou um *site* de hospedagem.

Users: ou usuarios, é o termo que define a audiência do mundo virtual e refere-se àqueles que se utilizam de petrechos informáticos.

Virtual: expressão que significa a simulação de situações reais sob novo enfoque. Apesar de não ser a única interpretação, consideramos que o enfoque neste trabalho é exclusivamente através do uso da tecnologia informática.

Virus: um programa que se replica em sistemas informáticos e se incorpora nos programas existentes, causando desde lentidão, até destruição de dados.

VoIP: abreviatura da expressão “*Voice Over Internet Protocol*” (Voz sobre protocolo de Internet), é a tecnologia que utiliza a linguagem da rede para conduzir a voz através de telefones. Assim, ao invés de a voz ser conduzida por cabos, ela é transformada em pacotes de dados que são enviados na velocidade da luz e que são novamente transformados em voz na máquina do destinatário.

Vulnerabilidade: Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Warez: expressão que primacialmente significa espertos que se especializam em quebrar a segurança de programas, liberando o uso livre ilegalmente.

Web 2.0: também denominada rede se segunda geração ou, ainda, rede colaborativa, representou a segunda geração de aplicativos de Internet em que o usuario não seria somente destinatário passivo mas também ativo, podendo contribuir para a construção da arquitetura e dos produtos e serviços no ciberespaço.

Website: é virtualmente um local representado por um endereço eletrônico, situado na rede mundial de computadores, que pode ser acessado por usuarios e onde estão armazenados arquivos e materiais e que podem ser dispostos para uso e visualização. É um meio de divulgação e de mídia.

Webcam: câmera de baixa qualidade de resolução, instalada em aparatos informáticos e que servem para tirar fotos, gravar vídeos ou simplesmente enviar imagens ao vivo e que pode ser utilizada na rede, inclusive para tornar as relações humanas mais realísticas.

Wi-fi: também conhecido como 802.11, utiliza-se de tecnologia sem fio através da qual usuarios podem se conectar na rede, com pequena cobertura (cerca de 30 metros quadrados) e alcance a partir de pulsos ondas de rádio

Wi-Max: tecnologia sem fio de alta velocidade através da qual usuarios podem se conectar na rede, com grande cobertura (cerca de 30 quilômetros quadrados) e alcance a partir de sinais emitidos por antenas

Window: compreendido como um quadro retangular na tela do computador ou do dispositivo informático, através da qual se pode acessar o conteúdo gráfico e interagir com ele. Também é o nome do sistema operacional produzido pela empresa Microsoft.

Wireless: com tradução como sendo “sem fio”, é a tecnologia de comunicação que dispensa o uso de fios e cabos

WWW: significando “*World Wide Web*” ou rede mundial ampla, é a coletânea de páginas com conteúdo gráfico (multimedia) que podem ser lidas e nelas se pode interagir através do uso de computadores ou dispositivos informáticos.

Worm: abreviatura de “*write once, read many*” (escreva uma vez, leia muitas), é um progrma de computador capaz de replicar-se muitas vezes, assim como um vírus

BIBLIOGRAFIA

ADAMS, James. Virtual defense. *Foreign Affairs*. New York, v.80, n.3, p.98-112, mai./jun. 2001.

AKEGAWA, Rita de Cássia Dias. Crime de informática: o envio de SPAM. *Cidadania e Justiça*. Ituiutaba, a.6, n.12, p.95-98, jul./dez. 2003.

ALBUQUERQUE, Roberto Chacon de. Lavagem de dinheiro nas operações financeiras veiculadas pela internet. *Revista de Direito Bancário e do Mercado de Capitais*. São Paulo, v.7, n.23, p.397-414, jan./mar. 2004.

ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo: Juarez de Oliveira, 2006.

ANDRÉS BERTONI, Eduardo. El derecho penal mínimo y la víctima. *in*: ROXIN, Claus. *et al. De los Delitos y de las Víctimas*. Buenos Aires: AD-HOC, 2001. p. 253-259.

ANDRÉS PALAZZI, Pablo. Delitos informáticos a través de Internet en la República Argentina. *Revista Brasileira de Ciências Criminais*. São Paulo, v.11, n.44, p.63-70, jul./set. 2003.

ANDRÉS PALAZZI, Pablo. Derecho penal informático: breve comentario a los legislativos sobre delitos informáticos. *Revista de Derecho Penal y Procesal Penal*. Buenos Aires, fasc.8, p.1525-1538, ago. 2006.

ANDREUCCI, Ricardo Antonio. *Legislação Penal Especial*. 2.ed.rev.atual. e aum. São Paulo: Saraiva, 2006.

ANIYAR DE CASTRO, Lola. *Criminologia da Libertação*. (Coleção pensamento criminológico, 10). Tradução de Sylvia Morentzohn. Rio de Janeiro: Revan, 2005.

ANIYAR DE CASTRO, Lola. *Pensamento Criminológico*: resumo gráfico e seu reflexo institucional: da criminologia clássica à criminologia dos direitos humanos. BH: Mandamentos, 2004.

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. *Jus Navegandi*. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=2250>>.

ARMAZA GALDOS, Julio. La eximente por consentimiento del titular del bien jurídico. *Revista Peruana de Ciencias Penales*, a.3, n.5, p.71-92, jan./jun. 1995.

ASCENSÃO, José de Oliveira. *Estudos Sobre Direito da Internet e da Sociedade da Informação*. Coimbra: Almedina, 2001.

ATHENIENSE, Alexandre. A jurisdição no ciberespaço. *Revista CEJ*. Brasília, v.7, n.20,

p.74-81, mar. 2003.

BARATTA, Alessandro. *Criminologia Crítica e Crítica do Direito Penal*: introdução à sociologia do Direito Penal. Tradução de Juarez Cirino dos Santos. 3.ed. (Coleção Pensamento Criminológico, 1). Rio de Janeiro: Revan, 2002.

BARBOSA, Marcelo Fortes. O consentimento do ofendido. *Revista dos Tribunais*. São Paulo, v.84, n.718, p.347-348, ago. 1995.

BARJA DE QUIROGA, Jacobo López. El moderno derecho penal para una sociedad de riesgos. *Poder Judicial*. Madrid, n.48, p.289-321, 1997.

BECCARIA, Cesare. *Dos Delitos e das Penas*. São Paulo: Martin Claret, 2005.

BERISTAIN, Antonio. *Derecho Penal, Criminología y Victimología*. Curitiba: Juruá, 2007.

BERISTAIN, Antonio. Notas sobre victimología: desde la victimología de mínimos hacia la victimología de máximos. *Cuadernos de Política Criminal*. Madrid, n.85, p.255-258, 2005.

BITENCOURT, Cezar Roberto. *Falência da Pena de Prisão*: causas e alternativas. 3.ed. São Paulo: Saraiva, 2004.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: parte geral. São Paulo: Saraiva, 2007, v.1.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: parte especial. 4.ed. São Paulo: Saraiva, 2008, v.3.

BITTAR, Walter Barbosa (coord.). *A Criminologia no Século XXI*. Rio de Janeiro: Lumen Juris, 2007.

BITTENCOURT, Edgar de Moura. *Vítima*. 3.ed. São Paulo: Leud, 1987.

BLUM, Renato M. S. Opice (coord). *Direito Eletrônico*: a internet e os tribunais. São Paulo: Edipro, 2001.

BLUM, Rita Ferreira. *Direito do Consumidor na Internet*. São Paulo: Quartier Latin, 2002.

BOVINO, Alberto. La participacion de la victima en el procedimiento penal. *Revista Brasileira de Ciencias Criminais*. São Paulo, v.6, n.21, p.417-438, jan./mar. 1998.

BRAVO, Otavio. O consentimento do ofendido na teoria do direito e na teoria da pena. *Direito em Movimento*. Instituto Capixaba de Estudos, v.2, p. 196-216, 2000.

BRUNO, Aníbal. *Comentários ao Código Penal*. Rio de Janeiro: Forense, 1969.

BUENO ARUS, Francisco. La atención a la víctima del delito. *Actualidad Penal*. Madrid, n.27, p.299-314, jul. 1990.

BUENO ARUS, Francisco. La posición de la víctima en el moderno sistema penal. *Boletim da Faculdade de Direito*. Coimbra, v.70, p.369-387, 1994.

CADERNO JURÍDICO. *Teoria da Imputação Objetiva e Teoria do Domínio do Fato*. São Paulo: Escola Superior do Ministério Público de São Paulo. a.1, n.1, abr. 2001.

CADERNO JURÍDICO. *Direito e Internet*. São Paulo: Escola Superior do Ministério Público de São Paulo. a.2, n.4, jul. 2002.

CALHAU, Lélio Braga. *Vítima e Direito Penal*. 2.ed. Belo Horizonte: Mandamentos, 2003.

CALLEGARI, André L. *et al*; GIACOMOLLI, Nereu J; CALLEGARI, André L. (coords.). *Direito Penal e Funcionalismo*. Tradução de André L. Callegari; Nereu J. Giacomolli; Lúcia Kalil. Porto Alegre: Livraria do Advogado, 2005.

CÂMARA, Guilherme C. *Programa de Política Criminal: orientado para a vítima de crime*. Co-edición Coimbra Editora e Revista dos Tribunais, 2008. 393p.

CAMEROM, Ben. Jurisdiction and the internet. *Law and Technology*. Washington D.C, v.34, n.2, p.1-17, 2001.

CANCINO MORENO, Antonio Jose. El consentimiento en materia penal. *Derecho Penal y Criminología*. Bogotá, v.12, n.40, p.33-81, jan./abr. 1990.

CANCIO MELIÁ, Manuel. La exclusión de la tipicidad por la responsabilidad de la víctima. *Revista de Derecho Penal y Criminología*. Madrid, n.2, p. 49-99. 1998.

CANCIO MELIÁ, Manuel. Reflexiones sobre la victimodogmática en la teoría del delito. *Revista Brasileira de Ciencias Criminais*. São Paulo, v.7, n.25, p.23-57, jan./mar. 1999.

CANCIO MELIÁ, Manuel. *Conducta de La Víctima e Imputación Objetiva en Derecho Penal: estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas*. 2.ed. Barcelona: J.M. Bosch, 2001.

CANCIO MELIÁ, Manuel; PEÑARANDA RAMOS, Enrique. Conducta de la víctima, delito imprudente y medición de la pena. *Jurisprudência Anotada*. Buenos Aires, fasc.7, p.237-247, 2005.

CAPEZ, Fernando. *Curso de Direito Penal: parte geral*. 9.ed.rev. e atual. São Paulo: Saraiva, 2005, v.1.

CAPEZ, Fernando. *Curso de Direito Penal: parte especial*. 5.ed.rev. e atual. São Paulo:

Saraiva, 2005, v.2.

CARUSO, Carlos A. A.; STEFFEN, Flávio D. *Segurança em Informática e de Informações*. 2.ed.rev. e ampl. São Paulo: SENAC São Paulo, 1999.

CARVALHO, Ivan Lira de. A internet e o acesso à justiça. *Revista de Processo*. São Paulo, v.25, n.100, p.107-126, out./dez. 2000.

CARVALHO, Salo. *Antimanual de Criminologia*. 2.ed. Rio de Janeiro: Lumen Juris, 2008.

CASAS BARQUERO, Enrique. La importancia del consentimiento en la teoria general del delito. *Doctrina Penal: teoria y practica en las ciencias penales*. Buenos Aires, v.11, n.42, p.213-230, abr./jun. 1988.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade*. Tradução de Maria Luiza X. de A. Borges; revisão técnica Paulo Vaz. Rio de Janeiro: Jorge Zahar Editor, 2003.

CASTELLS, Manuel. *A Sociedade em Rede*. Tradução de Jussara Simões. 6.ed. (A Era da Informação: economia, sociedade e cultura, 1). São Paulo: Paz e Terra, 1999.

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

CERT.BR. *Cartilha de Segurança para Internet*. Versão 3.1. Disponível em: <<http://cartilha.cert.br/>>.

CHURCH, Ray Everett. The Spam that Started it All. *Revista Eletrônica WIRED*. Disponível em: <<http://www.wired.com/politics/law/news/1999/04/19098>>

CONVENTION ON CYBERCRIME. Número 185, 23 de novembro 2001. Budapest. Disponível em: <<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>>.

COOTER, Robert; ULEN, Thomas. *Law and Economics*. 4.ed. New York: Addison Wesley, 2004

COSTA JÚNIOR, Paulo José da. *Curso de Direito Penal*. 2.ed. São Paulo: Saraiva, 1992.

COSTA JÚNIOR, Paulo José da. *O Direito de Estar Só: tutela penal da intimidade*. 4.ed.rev. e atual. São Paulo: Revista dos Tribunais, 2007.

COSTA, Álvaro Mayrink da. Crime informático. *Revista da EMERJ*. Rio de Janeiro. v.7, n.28, p.27-40, 2004.

COSTA, Ligia Maura. *Internet: guia bibliográfico comparado*. São paulo: Ieditora, 2002.

COVAS, Silvanio. O contrato no ambiente virtual: contratação por meio de informática. *Revista de Direito Bancário e do Mercado de Capitais*. São Paulo, v.2, n.5, p.100-122, mai./ago. 1999.

CRUZ, Danielle da Rocha. *Criminalidade Informática: tipificação penal das condutas ilícitas realizadas com cartões de crédito*. Rio de Janeiro: Forense, 2006.

D'URSO, Luíz Flávio Borges (coord.). *Justiça Criminal e Sociedade: 3º. encontro nacional dos advogados criminalistas*. São Paulo: Juarez de Oliveira, 2000.

D'ANDRÉA, Edgar Roberto Pacheco (coord.) *et al. Segurança em Banco Eletrônico*. São Paulo: PricewaterhouseCoopers, 2000.

DALL'AGLIO, Edgardo Jorge. El consentimiento y los vicios de la voluntad en los contratos concluídos por computador. *Revista del Colegio de Abogados de Buenos Aires*. Buenos Aires, v.49, n.1, p.79-85, mai. 1989.

DANNECKER, Gerhard; BASCÓN GRANADOS, Carmen. Sanciones contra la violación de los derechos de autor en las bases de datos. *Poder Judicial*. Madrid, n.53, p.107-126, 1999.

DELMANTO, Celso *et al. Código Penal Comentado*. 6.ed.atual. e ampl. Rio de Janeiro: Renovar, 2002

DIAS, Roberto. E.business, e.commerce, e.bank, e.broker... e.enforcement: uma desafio para a CVM. *Revista da CVM*. Rio de Janeiro, n.32, p.62-71, set. 2000.

DONATHEY, M. Scott. Dispute resolution in cyber space. *Journal of International Arbitration*. Geneve, v.15, n.4, p.127-168, dez. 1998.

DOTTI, Rene Ariel. O problema da vítima. *Revista dos Tribunais*. São Paulo, v.78, n.648, p.259-264, out. 1989.

D'URSO, Luiz Flávio Borges. *Direito Criminal na Atualidade*. São Paulo: Atlas, 1999.

ECO, Umberto. *Como se Faz uma Tese*. Tradução de Gilson Cesar Cardoso de Souza. 20.ed. São Paulo: Perspectiva, 2005.

ELIAS, Paulo Sá. Alguns aspectos da informática e suas consequências no direito. *Revista dos Tribunais*. São Paulo, v.88, n.766, p.491-500, ago, 1999.

ESTEVA, Margarita B. *La Víctima del Delito* (La autopuesta en peligro como causa de exclusión del tipo de injusto). Madrid: McGraw-Hill, 1999.

FEIJÓO SÁNCHEZ, Bernardo. ¿Imputación objetiva a la víctima que provoca a su agresor?. in: BARJA DE QUIROGA, Jacobo López; ZUGALDÍA ESPINAR, José Miguel

(coords.) *Dogmática y Ley Penal*. Madrid, Barcelona: Marcial Pons, Ediciones Jurídicas y Sociales, S.A. 2004. v.1, p.233-252.

FERNANDES NETTO, Antonio Joaquim. Responsabilidade do provedor Internet. *Ajuris: Revista da Associação dos Juizes do Rio Grande do Sul* (edição especial). Porto Alegre, n.2, p.551-561, mar. 1998.

FERNANDES, Antônio Scarance. *O Papel da Vítima no Processo Criminal*. São Paulo: Malheiros Editores, 1995. 253p.

FERREIRA, Ivette Senise; BAPTISTA, Luiz Olavo (coords.). *Novas Fronteiras do Direito na Era Digital*. São Paulo: Saraiva, 2002

FONTANA, Milton. Vítima e justiça penal: o processo da vitimização do ofendido. *Estudos Juridicos*. São Leopoldo, v.27, n.70, p.21-35, mai./ago. 1994.

FOUCAULT, Michel. *Vigiar e Punir: Nascimento da prisão*. 11.ed. Petrópolis: Vozes, 1994.

FRANCO, Alberto Silva. *et al. Justiça Penal Portuguesa e Brasileira: tendências de reforma: colóquio em homenagem ao Instituto Brasileiro de Ciências Criminais*. Org. Instituto Brasileiro de Ciências Criminais, 1.ed., São Paulo, 2008.

FRANCO, Alberto Silva. *Código Penal e sua Interpretação Jurisprudencial*. 6.ed. São Paulo: Revista dos Tribunais, 1997.

FREITAS, Mauricio Lopez. A participação da vítima nos crimes. *Revista do Ministério Público do Estado da Bahia: Serie Academica*. Salvador, v.1, n.1, p.200-213, jan./dez. 1998.

FROOMKIN, A. Michael. Habermas@discorse.net: toward a critical theory of cyberspace. *Harvard Law Review*. Cambridge, v.116, n.3, p.749-873, jan. 2003.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*. Brasília, v.7, n.20, p.67-73, mar. 2003.

GANDELMAN, Silvia Regina Dain. A propriedade intelectual na era digital: a difícil relação entre a internet e a lei. *BLA: Boletim Legislativo*. Rio de Janeiro, v.30, n.28, p.965-967, out. 1996.

GARCIA, Basileu. *Instituições de Direito Penal*. 3.ed. São paulo: Max Limonad, 1956.

GARCÍA, María José Segura. El consentimiento del sujeto pasivo en los delitos contra bienes jurídicos individuales. In: ZUGALDÍA ESPINAR, José Miguel; BARJA DE QUIROGA, Jacobo López (coords.) *Dogmática y Ley Penal: libro homenaje a Enrique Bacigalupo*. Madri: Marcial Pons, 2004. v.1, p.827-866.

GARCÍA-CERVIGÓN, Josefina García. El papel de la víctima en la política criminal especial: especial referencia al delito de lesiones. *Revista de Derecho Penal y Criminología*. (segunda época). Madrid, n. 2, p.483-500, 2004.

GARCÍA-PABLOS DE MOLINA, Antônio. *Criminologia*. 5.ed.rev, tradução de Luiz Flávio Gomes. São Paulo: Revista dos Tribunais, 2006.

GARRIDO, Vicente. *La Mente Criminal: la ciencia contra los asesinos en serie*. 2.ed., Madrid: Ediciones Temas de Hoy, 2007.

GASPARIAN, Tais. Privacidade em tempos de internet. *Revista do Advogado*. São Paulo, v.23, n.69, p.37-46, mai. 2003.

GATIEN, Konrad. How encryption and national security will affect the future of digital film distribution. *Southwestern Journal of Law and Trade in the Americas*. Los Angeles, v.8, n.1, p.229-249, 2001-2002.

GAVIRIA LONDONO, Vicente Emilio. La victima del delito en el proceso penal. *Derecho Penal y Criminologia*. Bogota, v.16, n.53, p.29-42, mai./ago. 1994.

GERACI, Danna. Spam: Opt in if you like. *Law and Technology*. Washington D.C, v.34, n.2, p.18-25, 2001.

GIBBS, W. Wayt. Computadores com desconfiômetro. *Scientific American*. São Paulo, a.3, n.33, p.47-53, fev. 2005.

GIL, Antonio de Loureiro. *Fraudes Informatizadas*. 2.ed. São Paulo: Atlas, 1999.

GOMES JUNIOR, Luiz Manoel. O controle jurisdicional das mensagens veiculadas através da internet. *Revista dos Tribunais*. São Paulo, v.86, n.738, p.75-82, abr. 1997.

GOMES, Alessandra Aparecida Calvoso. Operações bancárias via internet (internet banking) no Brasil e suas repercussões jurídicas. *Revista dos Tribunais*. São Paulo, v.92, n.816, p.94-108, out. 2003.

GONZALEZ DE MURILLO, José Luis Serrano. La duda de la víctima como forma de error en el delito de estafa. *Cuadernos de Política Criminal*. Madrid, n.50, p.529-547, 1993.

GRECO, Alessandra Orcesi Pedro. *A Autocolocação da Vítima em Risco*. (Ciência do Direito Penal Contemporâneo, 7). São Paulo: Revista dos Tribunais, 2004.

GRECO, Luis. *Um Panorama da Teoria da Imputação Objetiva*. Rio de Janeiro: Lumen Juris, 2005.

GRECO, Marco Aurelio; MARTINS, Ives Gandra da Silva (coords.). *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo: Revista dos Tribunais, 2001.

GROSSFELD, Bernhard. Global accounting: where internet meets geography. *The American Journal of Comparative Law*. Berkeley, v.48, n.2, p.261-306, 2000.

GUEIROS JUNIOR, Nehemias. O direito autoral e a evolução da tecnologia. *BLA: Boletim Legislativo*. Rio de Janeiro, v.30, n.12, p.381-383, abr. 1996.

GUERRERO MATEUS, María Fernanda. La ciberdelicuencia: la ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso colombiano. *Revista de Derecho Privado*. Santa Fé de Bogotá, v.16, n.29, p.37-121, dez. 2002.

HACHIGIAN, Nina. China's cyber-strategy. *Foreign Affairs*. New York, v.80, n.2, p.118-133, mar./abr. 2001.

HANDA, Sunny. Copyright liability when browsing on the information highway. *Law and Technology*. Washington, v.29, n.1, p.11-34, 1996.

HARTZOG, Neal. The magic lantern revealed: a report of the FBI's new key logging trojan and analysis of its possible treatment in a dynamic legal landscape. *Law and Technology*. Washington, v.35, n.1, p.1-42, 2002.

HASSEMER, Winfried. *Introdução aos Fundamentos do Direito Penal*. Tradução de Pablo Rodrigo Alfen da Silva. Porto Alegre: Sergio Antonio Fabris Editor, 2005.

HASSEMER, Winfried; CONDE, Francisco Muñoz. *Introdução à Criminologia*. Tradução, apresentação e notas de Cíntia de T. M. Chaves. Rio de Janeiro: Lumen Juris, 2008.

HEFENDEHL, Roland. ¿Debe ocuparse el derecho penal de riesgos futuros? Bienes jurídicos colectivos y delitos de peligro abstracto. Tradução de Eduardo Salazar Ortuño. *Anales de Derecho*. Murcia, n.19, p.147-158, 2001. Disponível em: <http://criminet.ugr.es/recpc/recpc_04-14.pdf>

HERRERA MORENO, Myriam. Notas criminológicas sobre los orígenes científicos de la victimología. *Cuadernos de Política Criminal*. Madrid, n.56, p.481-517, 1995.

HESPANHA, Benedito. O poder normativo da internet e a regulamentação dos crimes virtuais: uma análise crítica à legislação penal brasileira. *Justiça do Direito*. Passo Fundo, v.1, n.16, p.29-63, 2002.

HEY, Rau. Aspectos jurídicos da Internet. *Revista da ABPI*. Rio de Janeiro, n.19, p.2-40, nov./dez. 1995.

HEY, Raul. Design/informática/Internet e softwares: aspectos jurídicos. *Estudos Jurídicos*. São Leopoldo, v.30, n.78, p.5-15, jan./abr. 1997.

HOESCHL, Hugo Cesar. A liberdade de expressão na Internet. *Revista Trimestral de Jurisprudência dos Estados*. São Paulo, v.21, n.160, p.8-13, set./out. 1997.

HRUSCHKA, Joachim. La conducta de La víctima como clave para um sistema de los delitos patrimoniales que llevan consigo sustracción. *Anuario de Derecho Penal y Ciencias Penales*. Madrid, p. 453-466, 1999.

HURTADO POZO, José. El consentimiento en Derecho Penal Suizo. *Comentarios al Código Penal*. Suiza. p.531-547.

ISABEL GUERREIRO, Gabriela. La libertad de expresión y el derecho a la intimidad en internet. *Revista del Colégio de Abogados de la Plata*. La Plata, v.41, n.62, p.93-175, jan./dez. 2001.

JACCARD, Michel A. Securing copyright in transnational cyber space: the case for contracting with potential infringers. *Columbia Journal of Transnational Law*. New York, v.35, n.3, p.619-662, 1997.

JAKOBS, Günther, CANCIO MELIÁ, Manuel. *Direito Penal no Inimigo: noções e críticas*. Organização e tradução de André Luis Callegari; Nereu José Giacomolli. 3.ed. Porto Alegre: Livraria do Advogado, 2008.

JAKOBS, Günther. *A Imputação Objetiva no Direito Penal*. 2.ed.rev., tradução de André Luis Callegari. São Paulo: Revista dos Tribunais, 2007.

JAKOBS, Günther. *Fundamentos do Direito Penal*. Tradução de André Luís Callegari; Colaboração Lúcia Kalil. São Paulo: Revista dos Tribunais, 2003.

JEWKES, Yvonne. (ed.). *Crime Online*. Devon: Willan Publishing, Londres 2003.

JEWKES, Yvonne. (ed.). *Dot.cons: crime, deviance and identity on the internet*. Devon: Willan Publishing, 2003.

JOACHIM HIRSCH, Hans. Acerca de la posición de a víctima en el derecho penal y en el derecho procesal penal: sobre ls límites de las funciones jurídico-penales. Tradução de Júlio B.J Maier; Daniel R. Pastor. in: ROXIN, Claus. *et al. De los Delitos y de las Víctimas*. Buenos Aires: AD-HOC, p. 91-128, 2001.

JOACHIM SCHNEIDER, Hans. La posición juridical de la víctima del delito en el Derecho y en el Proceso Penal. *Doctrina Penal: teoría y práctica en las ciencias penales*. Buenos Aires, n.45-48, p.307-330, 1989.

JOSÉ AZAR, María. El consentimiento en la contratación de consumo por internet. *Revista de Direito do Consumidor*. São Paulo, v.11, n.42, p.27-47, abr./jun. 2002.

JUSTIÇA Penal : críticas e sugestões. São Paulo: Revista dos Tribunais, 1994.

KAMINSKI, Omar. A importância dos nomes na internet. *Revista CEJ*. Brasília, v.6, n.19, p.9-14, dez. 2002.

KENNEDY, Leslie W; SACCO, Vincent F. *Crime Victims in Context*. Oxford: Oxford University Press, 2007.

KIM, Jae-Young. Deregulation reconsidered: protecting internet speech in the United States, Germany, and Japan. *Communications and the Law*. Westport, v.24, n.1, p.53-75, mar. 2002.

KOSOVSKI, Ester (org.). *Vitimologia: enfoque interdisciplinar*. rev. e ampl. Rio de Janeiro: Reproart, 1994.

KOSOVSKI, Ester (org.); JUNIOR, Heitor Piedade (orgs.). *Vitimologia e Direitos Humanos*. Rio de Janeiro: Reproart, 2005.

KOSOVSKI, Ester. Fundamentos da vitimologia. *Âmbito Jurídico.com.br*. Disponível em: <http://www.sel.eesc.usp.br/informatica/graduacao/material/etica/private/fundamentos_da_vitimologia.pdf>.

KOSOVSKI, Ester; PIEDADE JUNIOR, Heitor; MAYR, Eduardo (coords.). *Vitimologia em Debate*. Rio de Janeiro: Forense, 1990.

KOSOVSKI, Ester; SÉGUIN, Elida (coords.). *Temas de Vitimologia*. Rio de Janeiro: Lumen Juris, 2000.

KRONE, Tony; JOHNSON, Holly. Internet purchasing: perceptions and experiences of Australian households. *Australian Institute of Criminology*. Canberra, n.330, fev. 2007. Disponível em: <<http://www.aic.gov.au/publications/tandi2/tandi330.html>>

LAVORENTI, Wilson; SILVA, José Geraldo Da. *Crime Organizado na Atualidade*. Campinas: Bookseller, 2000.

LAWAND, Jorge José. Direito Penal da internet: o advento de novos fatos típicos. *Revista Forense*. Rio de Janeiro, v.100, n.372, p.425-435, mar./abr. 2004.

LAZZARETTI, Andrea. Internet regulation and on-line gambling: a brief study of the US and EU legal system. *Law and Technology*. Washington, v.3, n.4, p.1-30, 1998.

LEMAN-LANGLOIS, Stéphane Leman. (ed.). *Technocrime: technology, crime and social control*. Devon: Willan Publishing, 2008.

LEVINE, John R.; BARROUDI, Carol. *Segredos da Internet*. Tradução ARX Publicações. São Paulo: Berkeley, 1996.

LIDSKY, Lyrrisa Barnett. Silencing John Doe: defamation and discourse in cyberspace. *Duke Law Journal*. Durham, v.49, n.2, p.855-946, fev. 2000.

LIMA, Gloria Regina Vianna ; JUNIOR, Heitor Piedade; SILVA, Luiz Alberto de Souza e;

ARAGÃO, Selma Regina. *Direito e Ordem*. Rio de Janeiro: Rabação, 1992.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. Campinas [SP]: Millennium Editora, 2005.

LOPES, Mauricio Antonio Ribeiro. *Princípio da Insignificância no Direito Penal*. 2.ed.rev. atual. ampl. São paulo: Revista dos Tribunais, 2000.

LOZA, Emile. Internet fraud: federal trade commission prosecutions of online conduct. *Communications and the Law*. Westport, v.23, n.2, p.55-98, mar. 2001.

LUCA, Heloisa Meroto de. O consentimento do ofendido à luz da teoria da imputação objetiva. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo, v.100, p.739-815, 2005.

LUCAS, Ana Cláudia Vinholes Siqueira. Vitimologia e vitimodogmática: uma abordagem 'garantista'. *Revista Transdisciplinar de Ciências Penitenciárias*. Pelotas, v.1, n.1, p.93-118, jan./dez. 2002.

LUCCA, Newton de; SIMIÃO FILHO, Adalberto (coords.) et al. *Direito & Internet: aspectos jurídicos relevantes*. Bauru, SP: EDIPRO, 2000.

LYNCH, Daniel C.; LUNDQUIST, Leslie. *Dinheiro Digital: o comércio na Internet*. Rio de Janeiro: Campus, 1996.

LYRA, Roberto. *Criminologia*. Rio de Janeiro: Forense, 1964.

MAGGS, Peter B. Consumer protection on the Internet. *Ajuris: Revista da Associação dos Juizes do Rio Grande do Sul* (edição especial). Porto Alegre, n.1, p.105-112, mar. 1998.

MALANDA, Sergio Romeo. La relevancia jurídico-penal de la conducta de la víctima en los delitos de estafa. in: JOACHIM HIRSCH, Hans; CAREZO MIR, José; ALBERTO DONNA, Edgardo (coords.). *Hans Welzel en el Pensamiento Penal de la Modernidad*. Buenos Aires: Culzoni Editores, Rubinzal-Culzoni, 2005. p.701-736.

MANUAL PRÁTICO DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

MANZANERA, Luis Rodrigues. *Victimología: estudios de la víctima*. México: Porrúa, 1988.

MARÍN, Boris Inga. Relevancia de La conducta de La víctima em el derecho penal. *Revista Peruana de Ciencias Penales* (edição especial). Peru, a.7-8, n.12, s.d., p. 502-509.

MARQUES, José Frederico. *Curso de Direito Penal : da infração penal*. São Paulo: Saraiva, 1954. v.2.

MARTINS, Flávio Alves. *Internet e Direito do Consumidor*. Rio de Janeiro: Lumen Juris, 2002.

MARZOCHI, Marcelo de Luca. Pornografia na internet. *Revista de Direito Administrativo*. Rio de Janeiro, v.233, p.229-243, jul./set. 2003.

MATEUCCI, Carlos Roberto Fornes. Privacidade e internet. *Revista de Direito Privado*. São Paulo, v.5, n.19, p.46-55, jul./set. 2004.

MCLEAN, Deckle. Internet defamation. *Communications and the Law*. Westport, v.24, n.4, p.21-41, dez. 2002.

MENDES, Antonio Jorge Fernandes De Oliveira. *Direito a Honra e a sua Tutela Penal*. Coimbra: Almedina, 1996.

MIRAGEM, Bruno. O conceito de domicílio e sua repercussão nas relações jurídicas eletrônicas: a aplicação da lei no espaço e a internet sob a perspectiva do direito brasileiro. *Revista de Direito Privado*. São Paulo, v.5, n.19, p.10-45, jul./set. 2004.

MITNICK, Kevin D.; SIMON, William L. *A Arte de Enganar*. Tradução Kátia Aparecida Roque; revisão técnica Olavo José Anchieschi Gomes. São Paulo: Pearson Makron Books, 2003.

MITNICK, Kevin D.; SIMON, William L. *A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos*. Tradução de Maria Lúcia G. L. Rosa; revisão técnica Julio César Pinto, Hoenir Ribeiro da Silva. São Paulo: Pearson Prentice Hall, 2005.

MIYAZAWA, Koichi; OHYA, Minoru. *Victimology in comparative perspective*. Tokyo: Seibundo Publishing, 1986.

MOLINA ARRUBLA, Carlos Mario. El consentimiento del sujeto pasivo de la infracción a la ley penal. *Revista de la Facultad de Derecho y Ciencias Políticas da Universidad Pontificia Bolivariana*. Medellín, n.75, p.11-38, out./dez. 1986.

MONITORAMENTO ELETRÔNICO. Sugestões para o controle de e-mails e recursos tecnológicos. São Paulo: FECOMERCIO, 2005.

MONROY VICTORIA, William. El consentimiento. *Derecho Penal y Criminología*. Bogotá, v.22, n.72, p.31-45, mai./ago. 2001.

MONTEIRO NETO, João Araújo. Crimes informáticos uma abordagem dinâmica ao direito penal informático. *Pensar*. Fortaleza, v.8, n.8, p.39-54, fev. 2003. Disponível em: <<http://www.unifor.br/notitia/file/1690.pdf>>

MONTEIRO, Cláudia S. *Filosofia do Direito: decisão judicial e teoria da argumentação*

jurídica. Florianópolis: Conceito Editorial, 2008.

MOREIRA FILHO, Guaracy. *Vitimologia: o papel da vítima na gênese do delito*. São Paulo: Jurídica Brasileira, 1999.

MOREIRA, José Carlos Barbosa. Pedofilia na Internet e o Estatuto da criança e do adolescente. *Revista Síntese de Direito Penal e Processual Penal*. Porto Alegre, v.2, n.8, p.5-8, jun./jul. 2001.

MOREIRA, Rômulo de Andrade. Globalização e crime. *Revista dos Tribunais*. São Paulo, v.92, n.811, p.469-496, mai. 2003.

MORÓN LERMA, Esther. *Internet y Derecho Penal: y otras conductas ilícitas en la red*. Pamplona: Aranzadi, 1999.

MOURA, Erika da Costa e Silva. O papel da vítima no Direito Penal e no processo criminal. *Revista do Ministério Público do Estado da Bahia: Série Acadêmica*. Salvador, v.1, n.1, p. 194-199, jan./dez, 1998.

NEGROPONTE, Nicholas. *A Vida Digital*. Tradução de Sérgio Tellaroli; supervisão técnica Ricardo Rangel. São Paulo: Companhia das Letras, 1995.

NEUMAN, Elías. *Victimología: el rol de la víctima en los delitos convencionales y no convencionales*. 2.ed.rev. e ampl. Buenos Aires: Editorial Universidad, 1994.

NIGRI, Deborah Fisch. Crimes informáticos: necessidade de regulamentação e controle. *BLA: Boletim Legislativo*. Rio de Janeiro, v.31, n.20, p.679-688, jul. 2007.

NOGUEIRA, Sandro D'Amato. *Vitimologia*. Brasília: Brasília Jurídica, 2006.

NORONHA, E. Magalhães. *Código Penal Brasileiro Comentado: crimes contra o patrimônio*. 2.ed.rev. e atual. São Paulo: Saraiva, 1958.

NUCCI, Guilherme de Souza. *Individualização da Pena*. 2.ed.rev.atual. e ampli. São Paulo: Revista dos Tribunais, 2007.

NUCCI, Guilherme de Souza. *Leis Penais e Processuais Penais Comentadas*. 3.ed.rev.atual. e ampli. São Paulo: Revista dos Tribunais, 2008.

NUCCI, Guilherme de Souza. *Manual de Direito Penal: parte geral: parte especial*. 3.ed.rev.atual. e ampli. São Paulo: Revista dos Tribunais, 2007.

NUÑEZ PAZ, Miguel Ángel. Reflexiones en torno a la relevância del consentimiento del sujeto pasivo en el artículo 143 del Código Penal. *Ediciones de la Universidad de Castilla-La Mancha*. Cuenca, p.433-454, 2001.

OLIVEIRA, Ana Sofia Schmidt de. *A vítima e o Direito Penal: uma abordagem do movimento vitimológico e de seu impacto no Direito Penal*. São Paulo: Revista dos Tribunais, 1999.

OLIVEIRA, Edmundo de. Vitimologia: tendência ou inclinação da vítima para o crime. *Revista Brasileira de Ciências Criminais*. São Paulo, v.9, n.36, p.351-369, out./dez. 2001.

OLIVEIRA, Edmundo. Novos rumos da vitimologia: o crime precipitado pela vítima. *Boletim Instituto Brasileiro de Ciências Criminais*. São Paulo, a.9, n.107, p.17, out. 2001.

OLIVEIRA, Edmundo. *Vitimologia e Direito Penal: o crime precipitado ou programado pela vítima*. Rio de Janeiro: Forense, 2003.

OLIVEIRA, Frederico Abrahão de. *Vítimas e criminosos*. Porto Alegre: Livraria do Advogado, 1993.

ORTS BERENGUER, Enrique; ROIG TORRES, Margarita. *Delitos Informáticos y Delitos Comunes Cometidos a través de la Informática*. Valencia: Tirant lo blanch, 2001.

ORWELL, George. 1984. Tradução de Wilson Velloso. 27.ed. São Paulo: Companhia Editora Nacional, 2002.

PAIVA, Mário Antônio Lobato de. A atipicidade dos delitos cometidos na internet. *Revista Síntese de Direito Penal e Processual Penal*. Porto Alegre, v.5, n.26, p.155-157, jun./jul. 2004.

PAIVA, Mário Antônio Lobato de. E-mail: prova obtida por meio ilícito. *Revista de Direito do Trabalho*. São Paulo, v.28, n.107, p.193-206, jul./set. 2002.

PARERAS, Luis G. *Título Internet y Derecho*. Barcelona: Masson, 1998.

PATTERSON, Chip. Copyright misuse and modified copyleft: new solutions to the challenges of Internet standardization. *Michigan Law Review*. Ann Arbor, v.98, n.5, p.1351-1383, mar. 2000.

PECK, Patricia. *Direito Digital*. São Paulo: Saraiva, 2002.

PIEIDADE JÚNIOR, Heitor. *Vitimologia: evolução no tempo e no espaço*. Rio de Janeiro: Freitas Bastos, 1993.

PIEIDADE JUNIOR, Heitor; KOSOVSKI, Ester. *Temas de Vitimologia II*. Rio de Janeiro: Lumen Juris, 2001.

PIERANGELI, José Henrique. *Crimes Contra a Propriedade Industrial e Crimes de Concorrência Desleal*. São Paulo: Revista dos Tribunais, 2003.

PIERANGELI, José Henrique. *O Consentimento do Ofendido: na teoria do delito*. 3.ed.rev. e atual. São Paulo: Revista dos Tribunais, 2001.

PRADO, Luiz Regis (coord.). *Responsabilidade Penal da Pessoa Jurídica: em defesa do Princípio da imputação penal subjetiva*. São Paulo: Revista dos Tribunais, 2001.

PRITCHARD, John. Información legal en la era electronica: internet y los nuevos sistemas de comunicación. *Revista Juridica de Catalunya*, número especial. 1895-1995. Barcelona, p.233-241, 1997.

PRITTWITZ, Cornelius. O direito penal entre direito penal do risco e direito penal do inimigo: tendências atuais em direito penal e política criminal. *Revista Brasileira de Ciências Criminais*. São Paulo, n.47, p.31-45, mar./abr. 2004.

PRITTWITZ, Cornelius. O direito penal entre direito penal do risco e direito penal do inimigo: tendências atuais em direito penal e política criminal. *Revista Brasileira de Ciências Criminais*. São Paulo, n.47, p.31-45, mar./abr. 2004.

PUGGINA, Marcio Oliveira. A erotização da infância na mídia e na internet. *Revista da AJURIS*. Porto Alegre, v.27, n.81, p.129-142, mar. 2001.

RAHAL, Flávia; GARCIA, Roberto Soares. Vírus, direito à intimidade e a tutela penal da internet. *Revista do Advogado*. São Paulo, v.23, n.69, p.25-36, mai. 2003.

RANGEL, Ricardo Melghior de Barros. *A Prova Ilícita e a Intercepção Telefônica no Direito Processual Penal Brasileiro*. Rio de Janeiro: Forense, 2000.

REALE JÚNIOR, Miguel. *Direito Penal Aplicado*. São Paulo: Revistas dos tribunais, 1992.

REINALDO FILHO, Demócrito Ramos. Crimes cometidos na internet: questões técnicas dificultam condenações. *Revista Síntese de Direito Penal e Processual Penal*. Porto Alegre, v.5, n.26, p.158-161, jun./jul. 2004.

REINALDO FILHO, Demócrito. Problemas decorrentes do uso de hiperlinks. *Revista CEJ*. Brasília, v.6, n.19, p.15-23, dez. 2002.

REYNA ALFARO, Luis M. Aproximaciones victimológicas al delito informático. *Revista de las Disciplinas del Control Social: Capítulo Criminológico*. Venezuela, v.31, n.4, p.93-104, Out./Dez. 2003.

RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na internet: uma primeira reflexão. *Revista de Direito do Consumidor*. São Paulo, v.11, n.41, p.151-165, jan./mar. 2002.

RIGONATTI, Sérgio Paulo (coord.), SERAFIM, Antonio de Padua e BARROS, Edgard Luis

de (orgs.). *Temas em Psiquiatria Forense e Psicologia Jurídica*. 1.ed. São Paulo: Editora Vetor, 2003.

RODRÍGUEZ MORALES, Coral. El internet y la protección del derecho a la intimidad. *Revista Jurídica de la Universidad de Puerto Rico*. Rio Piedras, v.72, n.4, 2003.

ROMEO CASABONA, Carlos Maria. El Consentimiento en las lesiones, en el proyecto de Código Penal de 1980. *Cuadernos de Política Criminal*. Madrid, n.17, p.263-295, 1982.

ROMERO COLOMA, Aurelia Maria. Las relaciones entre la victima y su agresor. *Actualidad Penal*. Madrid, n.13, p.177-185, mar./abr. 1993.

ROPERO CARRASCO, Julia. ¿Hay que "merecer" la protección del Derecho Penal?: derechos y deberes de las víctimas. *in: JORNADAS DE PROFESSORES Y ESTUDIANTES DE DERECHO PENAL DE LAS UNIVERSIDADES DE MADRID*. 9, 2005. *La Respuesta del Derecho Penal Ante los Nuevos Retos*. Madrid: s.e., pp. 115-136.

ROSSINI, Augusto Eduardo de Souza. Do necessário estudo do Direito Penal ante a informática e a telemática. *Revista Brasileira de Ciências Criminais*. São Paulo, v.12, n.49, p.39-47, jul./ago. 2004.

ROSSINI, Augusto Eduardo de Souza. *Informática, Telemática e Direito Penal*. São Paulo: Memorial Jurídica, 2004.

ROXIN, Claus. *A Proteção de Bens Jurídicos como Função do Direito Penal*. Organização e tradução de André Luís Callegari, Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2006.

ROXIN, Claus. *Estudos de Direito Penal*. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2006.

ROZO, Julio E.. La eficacia del consentimiento del sujeto pasivo. *Revista de la Academia Colombiana de Jurisprudencia*. Bogota, n.311, jun. 1998.

SÁ, Alvino Augusto de. *Criminologia Clínica e Psicologia Criminal*. São Paulo: Revista dos Tribunais, 2007.

SALDANHA, Ana Maria Pires. Vítima, uma personagem esquecida. *Revista Ibero-Americana de Ciências Penais*. Porto Alegre, a.2, n.3, p.11-18, mai./ago. 2001.

SALIMIPOUR, Negin. The challenge of regulating hate and offensive speech on the internet. *Southwestern Journal of Law and Trade in the Americas*. Los Angeles, v.8, n.2, p.395-421, 2001-2002.

SALVADOR NETTO, Alamiro Velludo. *Finalidades da Pena: Conceito material de delito e sistema penal*. São Paulo: Quartier Latin, 2009.

SALVADOR NETTO, Alamiro Velludo. *Tipicidade Penal e Sociedade de Risco*. São Paulo: Quartier Latin, 2006.

SANTOS, Juarez Cirino dos. *A Criminologia da Repressão*. Rio de Janeiro: Forense, 1979.

SARDAS, Letícia de Faria. Novos rumos no Direito Penal: os tipos penais e a internet. *Revista da EMERJ*. Rio de Janeiro, v.7, n.25, p.77-95, 2004.

SCHMALLEGER, Frank; PITTARO, Michel (eds.). *Crimes of the Internet*. 1.ed. Upper Saddle River, NJ: Prentice Hall, 2008.

SCHNEIER, Bruce. A Sci-Fi future awaits the court. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. A real remedy for phishers, 06/10/2005. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Real story of the rogue rootkit, 17/11/2005. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Anonymity won't kill the internet, 12/01/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Big risks come in small packages, 26/01/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Why VOIP needs crypto, 06/04/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Why Data Mining won't stop terror, 09/03/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. It's the economy, stupid, 29/06/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. The scariest terror threat of all, 15/06/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. The eternal value of privacy, 18/05/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. Everyone wants to "own" your PC, 04/05/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>.

_____. The problem of copycat cops, 08/03/2007. *Revista Eletrônica WIRED*.

Disponível em: <http://www.wired.com/politics/security>

_____. Vigilantism is a poor response to cyberattack, 05/04/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Why the human brain is a poor judge of risk, 22/03/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. How security companies sucker us with lemons, 19/04/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Do we really need a security industry? 03/05/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Portrait of the modern terrorist as an idiot, 14/06/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Why smart cops do dumb things, 22/02/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. What our top spy doesn't get: security and privacy aren't opposites, 24/01/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Steal this Wi-Fi, 10/01/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Secure passwords keep you safer, 11/01/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Google's click-fraud crackdown, 13/07/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Why everyone must be screened, 05/10/2006. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Why "anonymous" data sometimes isn't, 03/12/2007. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. When the internet is my hard drive, should I trust third parties? 21/02/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. Inside the twisted mind of the security professional, 20/03/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. The difference between feeling and reality in security, 03/04/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

_____. The Myth of the “Transparent society”, 06/03/2008. *Revista Eletrônica WIRED*. Disponível em: <http://www.wired.com/politics/security>

SCHOUEIRI, Luis Eduardo (org.). *Internet: o Direito na era virtual*. Edição 2.ed. Rio de Janeiro: Forense, 2001.

SCHÜNNEMANN, Bernd. The Role of the Victim Within the Criminal Justice System: A Three-Tiered Concept. *Buffalo Criminal Law Review*. New York, v.3, n.1, p.33-49, 1999. Disponível em: <[http://wings.buffalo.edu/law/bclc/bclrarticles/3\(1\)/schuenemann.pdf](http://wings.buffalo.edu/law/bclc/bclrarticles/3(1)/schuenemann.pdf)>

SCORZELLI, Patricia. A Internet e suas relações com o direito. *Boletim de Doutrina ADCOAS*. Rio de Janeiro, v.2, n.6, p.194-199, jun. 1999.

SCORZELLI, Patrícia. *A Comunidade Cibernética e o Direito*. Rio de Janeiro: Lumen Juris, 1997.

SÉGUIN, Elida (coord.) *et al. Vitimologia no Terceiro Milênio*. Rio de Janeiro: Forense, 2004.

SEPAROVIC, Zvonimir Paul. *Victimology: studies of victims*. Zagreb: Milan Ramljack, 1985.

SERAFIM, Antonio de Pádua. Investigação psicológica da personalidade na conduta criminosa. *in*: RIGONATTI, Sergio Paulo; SERAFIM, Antonio de Pádua; BARROS, Edgar Luiz de. (Orgs.). *Temas em Psiquiatria Forense e Psicologia Jurídica*. São Paulo: Vetor Editora, 2003, v.1, p. 65-78.

SHECAIRA, Sérgio Salomão. *Criminologia*. 2.ed. São Paulo: Revista dos Tribunais, 2008.

SILVA JÚNIOR, Délio e. Crimes informáticos: sua vitimização e a questão do tipo objetivo. *in*: DÁVILA, Fabio Roberto; SOUZA, Paulo Vinicius Sporleder de (coords.). *Direito Penal Secundário: estudos sobre crimes econômicos ambientais, informáticos e outras questões*. São Paulo: Revista dos Tribunais; Coimbra [Portugal]: Coimbra Editora, 2006. V.2.

SILVA JÚNIOR, Délio Lins e. *Imputação Objetiva e a Conduta da Vítima*. Curitiba: Juruá, 2008.

SILVA JUNIOR, Ronaldo Lemos da; WAISBERG, Ivo (orgs.) *et al. Comércio Eletrônico*. São Paulo: Revista dos Tribunais, 2001.

SILVA NETO, Amaro Moraes e. O spam e o direito brasileiro. *Revista CEJ*. Brasília, v.6, n.19, p.46-61, dez. 2002.

SILVA NETO, Amaro Moraes. *Emails Indesejados à Luz do Direito*. São Paulo: Quartier Latin, 2002.

SILVA NETO, Amaro Moraes. *Privacidade na Internet: um enfoque jurídico*. 1.ed. São Paulo: EDIPRO, 2001.

SILVA SÁNCHEZ, Jesús María. La consideración del comportamiento de la víctima en la teoría jurídica del delito: observaciones doctrinales y jurisprudenciales sobre la victimodogmática. *Revista Brasileira de Ciências Criminais*. São Paulo, v.9, n.34, pp. 163-164, 2001.

SILVA SÁNCHEZ, Jesús-María. La consideración del comportamiento de la víctima en la teoría jurídica del delito: observaciones doctrinales y jurisprudenciales sobre la “víctimo dogmática”. *Revista Brasileira de Ciências Criminais*. São Paulo, ano 9, n.34, p.163-194, abr./jun. 2001.

SILVA SÁNCHEZ, Jesús-María. *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*. (Colección Estudios y debates em derecho penal, 1). Buenos Aires: Euros Editores, 2008.

SILVA, Ivan Luiz da. *Crime Organizado: aspectos jurídicos e criminológicos* (Lei nº 9.034/95). Belo Horizonte: Nova Alvorada Edições, 1998.

SOUZA, Carlos Affonso Pereira de. O progresso tecnológico e a tutela jurídica da privacidade. *Direito, Estado e Sociedade*. Rio de Janeiro, n.16, p.6-39, jan./jul. 2000.

SOUZA, Jose Guilherme de. A participação inconsciente de vítima menor em crime sexual. *Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios*. Brasília, v.2, n.4, p.156-178, jul./dez. 1994.

SOUZA, José Guilherme de. *Vitimologia e Violência nos Crimes Sexuais: uma abordagem interdisciplinar*. Porto Alegre: Safe, 1998.

SOUZA, Luciano Anderson de. *Expansão do Direito Penal e Globalização*. São Paulo: Quartier Latin, 2007.

SOUZA, Marcos Antônio Cardoso de. Aplicação da legislação brasileira no caso Napster. *Revista Forense*. Rio de Janeiro, v.99, n.365, p.381-389. jan./fev. 2003.

STANGELAND, Per. Criminología realista y el problema de las víctimas. in: CORCOY BIDASOLO, Mirentxu; RUIDIAZ GARCÍA, Carmen. *Problemas Criminológicos en las Sociedades Complejas*. Pamplona: Universidad Pública de Navarra, 2000. Pp. 129-158.

STIX, Gary. Os segredos mais bem guardados: a criptografia quântica passou da teoria para o laboratório e de lá para produtos reais. *Scientific American*. São Paulo, a.3, n.33, p.39-45, fev. 2005.

STUBER, Walter Douglas; FRANCO, Ana C. de Paiva. A Internet sob a ótica jurídica. *Revista dos Tribunais*. São Paulo, v.87, n.749, p.60-81, mar. 1998.

TIMM, Luciano Benetti. A prestação de serviços bancários via internet (home banking) e a proteção do consumidor. *Revista de Direito do Consumidor*. São Paulo, v.10, n.38, p.74-92, abr./jun. 2001.

TOLEDO, Francisco de Assis. *Principios Básicos do Direito Penal*. São Paulo: Saraiva, 1991.

TORON, Alberto Zacharias. Crimes na Internet. *IOB-Repertório de Jurisprudência: civil, processual, penal e comercial*. São Paulo, n.22, p.478-476, nov. 2000.

TORRES, Margarita. Algunos apuntes sobre la evolución histórica de la tutela jurídica de la víctima del delito. *Estudios Penales y Criminológicos*. Santiago de Compostela, n.22, p.153-308, 1999-2000.

TOURINHO FILHO, Fernando da Costa. *Manual de Processo Penal*. 9.ed.rev. e atual. São Paulo: Saraiva, 2007.

VERDELHO, Pedro. A reforma penal portuguesa e o cibercrime. *Revista do Ministério Público*. Lisboa, a.27, n.108, p.97-124, out./dez. 2006.

VIANNA, Túlio Lima. Dos crimes pela internet. *Revista do CAAP*. Belo Horizonte, a.5, n.9, p.367-385, 2000.

VIANNA, Túlio Lima. Hackers: um estudo criminológico da subcultura cyberpunk. *Mundo Jurídico*. Disponível em: http://www.mundojuridico.adv.br/sis_artigos/artigos.asp?codigo=217.

VIANNA, Túlio Lima. La era del control. Introducción crítica al derecho penal cibernético. *Ciencias Penales Contemporáneas*. Mendoza, a.4, n.7/8, p.529-552, 2005.

VON HENTING, Hans. *The Criminal and His Victim: studies in the sociobiology of crime*. New Haven: Yale University Press, 1948.

WALCACER, Fernando Cavalcanti (coord.). *Revista de Direito: da Associação dos Procuradores do Novo Estado do Rio de Janeiro*. Rio de Janeiro: Lumen Juris, 1999.

WALKLATE, Sandra (ed.). *Handbook of Victims and Victimology*. Devon: Willan Publishing, 2007.

WEBBER, Jason. Combating cyber-crime: at what cost?. *Law and Technology*. Washington D.C, v.34, n.2, p.26-33, 2001.

WILLIAMS, Matthew. Policing and cybersociety: the maturation of regulation within an

online community. *Policing e Society*. Abingdon, v.17, n.1, p. 59-82, mar. 2007.

ZAMORA AVILA, Martha Lucia. Tratamiento jurídico-penal de la puesta en peligro de la víctima con su consentimiento. *Derecho Penal y Criminología*. Bogota, v.13, n.44, p.37-56, mai./ago. 1991.

ZAMORA GRANT, Jose. Los modelos victimologicos. *Boletín Mexicano de Derecho Comparado*. Mexico, v.31, n.93, p.835-849, set./dez. 1998.

ZANELATO, Marco Antonio. Condutas ilícitas na sociedade digital. *Revista de Direito do Consumidor*. São Paulo, v.11, n.44, p.206-261, out./dez. 2002.

ZEFF, Robbin; ARONSON, Brad. *Publicidade na Internet*. Tradução de Tom Venetianer Rio de janeiro: Campus, 2000.

ZHAO, Yun. Internet service providers and their liability. *Law and Technology*. Washington D.C, v.34, n.1, p.1-19, 2001.