CRIMES NA INTERNET: elementos para uma reflexão sobre a ética informacional

Mário Furlaneto Neto
José Augusto Chaves Guimarães

RESUMO

Aduz que a reflexão sobre a dimensão ética contida nos novos espaços e suportes informacionais trazidos à realidade do profissional da informação exige seu deslocamento da tradicional abordagem da internet como um importante e valioso espaço de disponibilização de informações para, em uma visão mais ampla, discutir os entraves de ordem jurídica a que o uso inadvertido desse espaço pode levar.

Salienta, para tanto, os conceitos e as tipologias de crimes praticados "com" e "contra" o computador, ao concluir que os crimes informáticos não podem mais deixar de ser uma preocupação social, carecendo de tipificação em nosso ordenamento jurídico.

Aponta para a necessidade de uma reflexão ética, por parte dos profissionais da informação, a fim de poderem, de forma legítima, contribuir para que o acesso e a recuperação de informações se façam consoante a estrutura jurídica estabelecida, atuando não apenas como meros disponibilizadores de informações, mas como valiosos colaboradores das instâncias jurídicas que visam a garantir tais direitos.

PALAVRAS-CHAVE

Informática – crime; internet; ética profissional; informação.

1 INTRODUÇÃO

Em um momento pautado pelo fenômeno da globalização, quando a questão tecnológica passa a ser condição *sine qua non* para o desenvolvimento das atividades informacionais, mormente em se considerando uma realidade de clientes mais exigentes e interativos, cabe refletir sobre a dimensão ética que os novos espaços e suportes informacionais traz à realidade do profissional da informação, não raras vezes impactando sua ação.

Nesse contexto, Guimarães[1] refere-se a um conjunto de compromissos éticos a serem encarados na área informacional, dentre os quais se destacam questões como a qualidade dos serviços e produtos, o valor estratégico e social da informação, a confiabilidade da informação prestada e, em última análise a responsabilidade profissional que decorre de tais aspectos.

Se antes, quando a atividade informacional mais se ligava ao acesso a estoques e à entrega de pacotes (caracterizada por Guimarães[2], como a fase do *information delivery*), já se podia observar uma dimensão eminentemente jurídica (como a responsabilidade civil por danos causados ao usuário pela disseminação de informações desatualizadas ou incorretas), hoje, com o fenômeno internet, quando os conceitos de suporte e de meio passam a ser rediscutidos, e principalmente quando o volume informacional atinge dimensões nunca antes aventadas, não se pode mais fugir da reflexão sobre o aspecto criminal incidente na rede mundial, de modo a revelar um efetivo compromisso ético do profissional com a informação em si e com sua própria profissão[3].

Tal reflexão encontra ainda mais respaldo quando se discute o papel da informação jurídica como um bem social, notadamente ligada a segmentos do Poder Público que, por definição, devem zelar pelo respeito ao princípio da legalidade.

Desse modo, objetiva-se, no presente artigo, deslocar-se um tanto da tradicional abordagem da internet como um importante – e valioso espaço – de disponibilização de informações com agilidade para, em uma visão mais ampla, propiciar a reflexão acerca dos entraves de ordem jurídica a que o uso inadvertido desse espaço pode levar.

2 INTERNET: ELEMENTOS HISTÓRICOS

Fazendo uma digressão histórica sobre o surgimento da internet, Paesani[4] menciona que o projeto *Arpanet* da Agência de Projetos Avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, à *Rand Corporation* a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos.

Desse modo, a solução aventada foi a criação de pequenas redes locais (*LAN*), posicionadas nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (*WAN*). Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, esse conjunto de redes conexas – internet, isto é, *inter networking*, literalmente, coligação entre redes locais distantes, garantiria a comunicação entre as remanescentes cidades coligadas.

Posteriormente, no ano de 1973, *Vinton Cerf*, do Departamento de Pesquisa avançada da Universidade da Califórnia e responsável pelo projeto, registrou o Protocolo de Controle de Transmissão/Protocolo internet (protocolo *TCP/IP*), código que consentia aos diversos *networks* incompatíveis por programas e sistemas comunicarem-se entre si.

Assim decolou a internet, no auge do processo de barateamento das comunicações, hoje vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de tempo e lugar.

O mais importante elemento detonador dessa verdadeira explosão, que permitiu à internet transformar-se num instrumento de comunicação de massa, ressaltada por Paesani[5], a *world wide web* (ou www, w3, web ou simplesmente rede mundial), nasceu no ano de 1989, no Laboratório Europeu de Física, de altas energias, com sede em Genebra, sob o comando de T. Berners – Lee e R. Cailliau, composta por hipertextos, ou seja, documentos cujo texto, imagem e sons seriam evidenciados de forma particular e poderiam ser relacionados com outros documentos, permitindo que, com um simples clique no *mouse,* o usuário pudesse ter acesso aos mais variados serviços e informações, sem necessidade de conhecer os inúmeros protocolos de acesso.

Se, por um lado, incontestável é o avanço e os benefícios que o uso ético da internet trouxe para a propagação da informação, com benefícios incalculáveis em sua divulgação, por outro, têm-se os riscos inerentes à tecnologia da informatização, notadamente os crimes informáticos.

3 CRIMES INFORMÁTICOS: CONCEITUAÇÃO E TIPOLOGIA

Segundo Ferreira[6], o surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Würzburg, à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial.

A partir de 1980, ressalta a autora o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto. Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época.

Essa criminalidade, no entender de Gomes[7], conta com as mesmas características da informatização global: *transnacionalidade – todos os países fazem uso da informatização (qualquer que seja o seu desenvolvimento econômico, social ou cultural); logo, a delinqüência correspondente, ainda que em graus distintos, também está presente em todos os continentes; universalidade – integrantes de vários níveis sociais e econômicos já têm acesso aos produtos*

informatizados (que estão se popularizando cada vez mais); ubiqüidade – a informatização está presente em todos os setores (públicos e privados) e em todos os lugares.

Nesse contexto, observa-se que, como fator criminógeno, cabe reconhecer que a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais (estelionato, por exemplo). Há, assim, crimes cometidos com o computador (*The computer as a tool of a crime*) e os cometidos contra o computador, isto é, contra as informações e programas nele contidos (*The computer as the object of a crime*).

Uma primeira abordagem da questão é desenvolvida por Corrêa[8], no contexto dos denominados "crimes digitais", ou seja, *todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar.*

Pode-se observar que, em tal conceituação, o autor enfatiza os crimes cometidos contra o computador, ou seja, contra as informações e programas nele contidos, bem como contra as informações ou dados em trânsito por computadores, com o dolo específico de ameaça e de fraude, não abordando aqueles crimes praticados com o computador, mas cujo bem protegido pelo ordenamento jurídico é diverso, como por exemplo, a pedofilia.

Em outra corrente, Pinheiro[9] classifica crimes informáticos ou cibernéticos em virtuais puros, mistos e comuns.

O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *homebanking* ou no chamado *salami-slacing*, onde o *cracker* retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil (art. 241 do ECA) era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por *e-mail* entre pedófilos e divulgação em *sites*. Mudou a forma, mas a essência do crime permanece a mesma.

A partir de 1980, ressalta a autora o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto. Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época.

De forma abrangente, Ferreira[10] define crime de informática como sendo *toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão*.

A autora segue justificando o conceito de ação como comportamento humano comissivo ou omissivo que corresponda ao modelo previsto em lei como crime (típico), com a respectiva penalidade, atendendo ao princípio da legalidade que norteia o Direito Penal, completando-se o conceito de crime se a conduta ilícita e a responsabilidade penal puder ser atribuída ao seu autor.

Indo ao encontro dos fatores criminógenos expostos por Gomes[11], por julgar mais compatível com a casuística, Ferreira[12] adota a classificação proposta por Hervé Croze e Yves Biscunth, para quem os crimes de informática se distinguem em duas categorias:

1) os atos dirigidos contra um sistema de informática, por qualquer motivo, verdadeiro núcleo da criminalidade informática, por se tratarem de ações que atentem contra o próprio material informático (suportes lógicos ou dados dos computadores);

2) os atos que atentem contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderiam todas as espécies de infrações previstas em lei penal.

Embora a expressão "conduta não-ética" inserida no contexto da definição seja incompatível com a cultura jurídica brasileira, por partir do pressuposto de que toda ação ou omissão prevista em norma penal incriminadora é indesejável, Rossini entende que *o melhor conceito para "delito informático" é o cunhado pela Organização para Cooperação Econômica e Desenvolvimento da ONU: "o crime de informática é qualquer conduta ilegal não-ética, ou não-autorizada, que envolva processamento automático de dados e/ou transmissão de dados"* [13].

Para o autor, há delitos informáticos puros, "em que o sujeito visa especificamente ao sistema de informática em todas as suas formas", incluindo *software*, *hardware*, dados e sistemas, bem como meios de armazenamento, e delitos informáticos mistos, "em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático", como por exemplo, a prática de homicídio por meio da internet, com a mudança a distância de rota de um avião[14].

Em uma abordagem sobre ilícitos informáticos que violam a privacidade na *web*, Rossini[15] cita, dentre outras condutas:

a) spamming, *como forma de envio não-consentido de mensagens publicitárias por correio eletrônico* a uma massa finita de usuários da rede, conduta esta não oficialmente criminal, mas antiética;

b) *cookies*, a quem chama "biscoitinhos da *web*", *pequenos arquivos de textos que são gravados no computador do usuário pelo* browser *quando ele visita determinados* sites *de comércio eletrônico*, de forma a identificar o computador com um número único, e obter informações para reconhecer quem está acessando o *site*, de onde vem, com que periodicidade costuma voltar e outros dados de interesse do portal;

c) *spywares*, como *programas espiões que enviam informações do computador do usuário da rede para desconhecidos*, de maneira que até o que é teclado é monitorado como informação, sendo que alguns *spywares* têm mecanismos que acessam o servidor assim que usuário fica *on-line* e outros enviam informações por *e-mail*;

d) *hoaxes*, como sendo *e-mails que possuem conteúdos alarmantes e falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais*, como as correntes ou pirâmides, *hoaxes* típicos que caracterizam crime contra a economia popular[16], podendo, ainda, estarem acompanhadas de vírus;

e) *sniffers*, programas espiões, assemelhados aos *spywares*, que, introduzidos no disco rígido, visam a rastrear e reconhecer *e-mails* que circundam na rede, de forma a permitir o seu controle e leitura;

f) *trojan horses* ou cavalos de tróia, que, uma vez instalados nos computadores, abrem suas portas, tornando possível a subtração de informações, como senhas, arquivos etc.

Sobre o cavalo de tróia, o autor complementa que *embora o usuário possa recebê-lo de várias maneiras, na maioria das vezes ele vem anexado a algum* e-mail*. Este vem acompanhado de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Uma vez aberto o arquivo, o trojan horse se instala no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos* hackers *o controle total da sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado.*

Considerando-se que boa parte dos computadores é dotada de microfones ou câmaras de áudio e vídeo, observa-se que o cavalo de tróia permite a possibilidade de se fazer escuta ambiente clandestina, arma poderosa nas mãos de criminosos que visam à captura de segredos industriais.

A doutrina juscibernética comparada, mormente a ibero-americana, enriquece ainda mais o debate.

Segundo os argentinos Levene e Chiaravalloti[17], não há uma definição de caráter universal própria de delito informático, apesar dos esforços dos *experts* que tenham se ocupado do tema, e, enquanto não existe a concepção universal, foram formulados conceitos funcionais atendendo a realidades nacionais concretas.

Desse modo, os autores resgatam o entendimento de María de la Luz Lima[18], segundo a qual *delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.* Complementando sua definição, classifica os delitos eletrônicos em três categorias:

a) Os que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais onde os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito;

b) Os que utilizam a tecnologia eletrônica como meio, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio; e

c) Os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objetivo de danificá-lo.

No *Oitavo Congresso sobre Prevenção de Delito e Justiça Penal*, celebrado em Havana, Cuba, em 1990, a Organização das Nações Unidas (ONU)[19] publicou uma relação de tipos de delitos informáticos. A relação reconheceu os seguintes delitos:

1. Fraudes cometidas mediante manipulação de computadores, caracterizadas por:

a) manipulação de dados de entrada, também conhecida como subtração de dados;

b) manipulação de programas, modificando programas existentes em sistemas de computadores ou enxertando novos programas ou novas rotinas;

c) manipulação de dados de saída, forjando um objetivo ao funcionamento do sistema informático, como, por exemplo, a utilização de equipamentos e programas de computadores especializados em decodificar informações de tarjas magnéticas de cartões bancários ou de crédito;

d) manipulação informática, técnica especializada que aproveita as repetições automáticas dos processos do computador, apenas perceptível em transações financeiras, em que se saca numerário rapidamente de uma conta e transfere a outra.

2. Falsificações informáticas:

a) como objeto, quando se alteram dados de documentos armazenados em formato computadorizado;

b) como instrumento, quando o computador é utilizado para efetuar falsificações de documentos de uso comercial, criando ou modificando-os, com o auxílio de impressoras coloridas a base de raio laser, cuja reprodução de alta qualidade, em regra, somente pode ser diferenciada da autêntica por perito.

3. Danos ou modificações de programas ou dados computadorizados, também conhecidos como sabotagem informática, ato de copiar, suprimir ou modificar, sem autorização, funções ou dados informáticos, com a intenção de obstaculizar o funcionamento normal do sistema, cujas técnicas são:

a) vírus, série de chaves programadas que podem aderir a programas legítimos e propagar-se a outros programas informáticos;

b) gusanos, análogo ao vírus, mas com objetivo de infiltrar em programas legítimos de programas de dados para modificá-lo ou destruí-lo, sem regenerar-se;

c) bomba lógica ou cronológica, requisitando conhecimentos especializados já que requer a programação para destruição ou modificação de dados em um certo momento do futuro;

d) acesso não-autorizado a sistemas de serviços, desde uma simples curiosidade, como nos casos de hackers, *piratas informáticos, até a sabotagem ou espionagem informática;*

e) piratas informáticos ou hackers, *que aproveitam as falhas nos sistemas de seguranças para obter acesso a programas e órgãos de informações; e*

f) reprodução não-autorizada de programas informáticos de

proteção legal, causando uma perda econômica substancial aos legítimos proprietários intelectuais.

Posteriormente, no *Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente*[20], *celebrado em Viena, entre os dias 10 e 17 de abril de 2000, a ONU publicou um comunicado à imprensa, relacionando outros tipos de delitos informáticos, praticados por meio do computador, quais sejam:*

a) Espionagem industrial: espionagem avançada realizada por piratas para as empresas ou para o seu próprio proveito, copiando segredos comerciais que abordam desde informação sobre técnicas ou produtos até informação sobre estratégias de comercialização;

b) Sabotagem de sistemas: ataques, como o bombardeiro eletrônico, que consistem no envio de mensagens repetidas a um site*, impedindo assim que os usuários legítimos tenham acesso a eles. O fluxo de correspondência pode transbordar a quota da conta pessoal do titular do* e-mail *que as recebe e paralisar sistemas inteiros. Todavia, apesar de ser uma prática extremamente destruidora, não é necessariamente ilegal;*

c) Sabotagem e vandalismo de dados: intrusos acessam sites *eletrônicos ou base de dados, apagando-os ou alterando-os, de forma a corromper os dados. Podem causar prejuízos ainda maiores se os dados incorretos forem usados posteriormente para outros fins;*

d) Pesca ou averiguação de senhas secretas: delinqüentes enganam novos e incautos usuários da internet *para que revelem suas senhas pessoais, fazendo-se passar por agentes da lei ou empregados de provedores de serviço. Utilizam programas para identificar senhas de usuários, para que, mais tarde, possam usá-las para esconder verdadeiras identidades e cometer outras maldades, como o uso não autorizado de sistemas de computadores, delitos financeiros, vandalismo e até atos de terrorismo;*

e) Estratagemas: astuciosos utilizam diversas técnicas para ocultar computadores que se parecem eletronicamente com outros para lograr acessar algum sistema geralmente restrito a cometer delitos. O famoso pirata Kevin Mitnick se valeu de estratagemas em 1996, para invadir o computador da casa de Tsotomo Shimamura, expert *em segurança, e destruir pela* internet *valiosos segredos de segurança;*

(...) crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. (...) Se antes, por exemplo, o crime como o de pornografia infantil (art. 241 do ECA) era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por *e-mail* entre pedófilos e divulgação em *sites*. (...)

f) Pornografia infantil: a distribuição de pornografia infantil por todo o mundo por meio da internet está aumentando. O problema se agrava ao aparecer novas tecnologias como a criptografia, que serve para esconder pornografia e demais materiais ofensivos em arquivos ou durante a transmissão;

g) Jogos de azar: o jogo eletrônico de azar foi incrementado à medida que o comércio brindou com facilidades de crédito e transferência de fundos pela rede. Os problemas ocorrem em países onde esse jogo é um delito e as autoridades nacionais exigem licenças. Ademais, não se pode garantir um jogo limpo, dado as inconveniências técnicas e jurisdicionais para sua supervisão;

h) Fraude: já foram feitas ofertas fraudulentas ao consumidor tais como a cotização de ações, bônus e valores, ou a venda de equipamentos de computadores em regiões onde existe o comércio eletrônico;

i) Lavagem de dinheiro: espera-se que o comércio eletrônico seja um novo lugar de transferência eletrônica de mercadorias e dinheiro para lavar as ganâncias do crime, sobretudo, mediante a ocultação de transações;

A rede mundial, uma sociedade virtual que modificou hábitos e costumes, combinando comportamentos tradicionais com o acesso à informação e cultura, também se tornou motivo de inquietude, um rico campo para as mais variadas atividades ilícitas, criminalidade esta, caracterizada pela dificuldade de investigação, prova e aplicação da lei penal, pelo caráter transnacional e ilimitado dessas condutas, o que pode gerar conflitos de Direito Internacional, em decorrência da competência da jurisdição sancionadora.

Em artigo sobre a regulamentação jurídica do fenômeno informático, Carrascosa López[21] diz que o novo Código Penal espanhol, aprovado pela Lei Orgânica n. 10, de 23 de novembro de 1995, conferiu um capítulo aos crimes informáticos, contemplando, dentre outras, as seguintes infrações penais: fraude informática (art. 248.2), utilização ilícita de cartões eletromagnéticos nos delitos de roubo (arts. 239 *in fine* c.c. o art. 238), violação informática (art. 256), dano e sabotagem informática (art. 264 e ss.), espionagem informática (art. 278 e ss.), violação da intimidade (art. 197 e ss.), propriedade intelectual (art. 270 e ss.), bem como pirataria de programas (art. 283).

Em recente revisão, o Código Penal espanhol foi atualizado pela Lei Orgânica n. 11, de 30 de abril de 1999[22], que contemplou como crimes a pornografia infantil praticada via internet e a posse de material pornográfico relacionado à pornografia infantil.

Como vimos, o computador pode ser meio para a prática de delitos previstos na legislação ordinária, como, por exemplo: ameaça (promessa de malefícios futuros); crimes contra a honra praticados via *e-mail* (ofensas à honra objetiva – difamação –, subjetiva – injúria – e a imputação falsa de fato considerado como crime – calúnia); violação de correspondência, considerando-se a confidencialidade da correspondência eletrônica; tráfico de drogas; apologia ao crime; e até mesmo homicídio doloso, na hipótese de uma pessoa, intencionalmente, interferir na programação de um aparelho em funcionamento em um paciente internado na Unidade de Terapia Intensiva (UTI), cujo desligamento venha a lhe causar a morte, bem como para outras condutas potencialmente danosas, ainda não-disciplinadas pelo Direito Penal.

Importante dizer que a caracterização do delito praticado por meio do computador dependerá da análise do caso concreto, devendo a con-

duta do delinqüente informático se subsumir em norma prevista na legislação em vigor do país onde o delito for cometido, sendo que a exemplificação neste artigo apresentada não tem o condão de ser taxativa.

Figura não-tipificada pelo Direito Penal brasileiro, o delito de terrorismo praticado com o auxilio da informática é classificado por Telles Valdés[23] da seguinte forma:

a) Terrorismo de Estado: praticado por governantes que, para poder seguir exercendo um controle político sobre seus governados, recorrem ao uso da informática como fator de opressão, de forma a utilizar em seu proveito a informação como poder. Distinguem-se governantes de Estados totalitários daqueles que estão sob o manto de um Estado democrático, que recorrem a essa estratégia para um melhor controle da cidadania. Para alguns tratadistas, essa conduta trata-se de excesso de poder e não de terrorismo, requerendo um contrapeso adequado para que não suscitem abusos contra os cidadãos, ou seja, um adequado controle sobre o controle, como, por exemplo, os desenvolvidos pelo Escritório de Inspeção de Dados da Suécia, a Comissão Federal de Dados da República Federativa da Alemanha e a Comissão Nacional de Liberdades e Informática da França;

b) Terrorismo entre Estados: caso em que a teleinformática a serviço de um determinado Estado pode propiciar verdadeiros atentados contra a soberania de outros Estados por intermédio do conhecimento e uso indevido de dados informacionais de caráter confidencial e estratégico, mediante o fluxo de dados transnacionais. Como exemplos temos eventuais ocupações físicas e destruição parcial ou total de centros de informação, como um quartel militar e uma central nuclear ou química;

c) Terrorismo entre particulares: na posição do autor, trata-se de atos de criminalidade em sentido lato, motivados por questões de ordem pessoal, histórica, econômica e religiosa. Cita como exemplo os vírus informáticos, que constituem, em algumas ocasiões, sempre que presente a intenção dolosa de causar um dano, verdadeiros atentados terroristas contra o suporte material e lógico dos computadores com a conseqüente perda de informações e, sobretudo, caracterizando mais prejuízos do que originalmente se pretendia provocar, inclusive financeiro e com perdas de vidas humanas, o que a doutrina tem considerado verdadeiros delitos preterintencionais[24].

d) Terrorismo de particulares contra o Estado: conduta esta mais conhecida na atualidade como realizada por grupos anárquicos de esquerda, de direita, fanáticos religiosos, ecologistas, etc. Geralmente provocam estragos de perdas humanas e materiais. Como exemplos, teríamos a possibilidade de uma invasão física e automatizada a algum centro informático ou a inserção de vírus informáticos, o planejamento e a simulação de atentados por meio de um computador a fim de aperfeiçoar o verdadeiro ataque, a posse de informações confidenciais (fitas, discos magnéticos ou qualquer outro suporte material de informação), ou a ação de roubos e fraudes informáticas para a obtenção de fundos para suas atividades etc.

4 CONCLUSÃO

Como se pode observar, a dimensão criminal ora verificada na internet não apenas conserva os aspectos tradicionalmente preconizados pelo Direito Penal, como traz à tona peculiaridades desse novo contexto. Assim, condutas igualmente lesivas, mas ainda não-consideradas crimes, por dependerem de regulamentação específica, como é o caso do dano praticado contra informações e programas contidos em computador, proliferam em ritmo acelerado, e por vezes incontrolável.

Desse modo, questões como a propagação deliberada de vírus informáticos, destruindo sistemas inteiros e levando à impossibilidade de acesso à informação (direito constitucionalmente protegido), não podem mais deixar de ser uma preocupação inerente ao profissional da informação, visto incorporarem-se a seu próprio fazer.

Portanto, uma reflexão ética a mais se incorpora ao *métier* desse profissional, qual seja, aquela de buscar, pelas formas que lhe forem legitimamente acessíveis, propiciar que o acesso e a recuperação de informações se façam em moldes consonantes com a estrutura jurídica estabelecida, atuando não apenas como um mero disponibilizador de informações, mas como um valioso colaborador das instâncias jurídicas que visam a garantir tais direitos.

NOTAS BIBLIOGRÁFICAS

1 GUIMARÃES, José Augusto Chaves. O profissional da informação sob o prisma de sua formação. *In:* VALENTIM, Marta Lígia Pomin (org.). *Profissionais da informação: formação, perfil e atuação profissional.* São Paulo: Polis, 2000. p. 66.

2 GUIMARÃES, *op. cit.*, p. 65.

3 GUIMARÃES, *op.cit.,* p. 66.

4 PAESANI, Liliana Minardi. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil*. São Paulo: Atlas, 2000. 141 p. p. 25.

5 Idem. p. 26.

6 FERREIRA, Ivette Senise. A criminalidade informática. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito e internet: aspectos jurídicos relevantes.* Bauru: Edipro, 2000. p. 207 – 237.

7 GOMES, Flávio Luiz. *Crimes informáticos.* Disponível em: <www.direitocriminal.com.br>. Acesso em 26 nov. 2000.

8 CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet.* São Paulo: Saraiva, 2000. 135 p. p. 43.

9 PINHEIRO, Reginaldo César. *Os crimes virtuais na esfera jurídica brasileira.* São Paulo: IBCCrim, v. 101, p. 18-19, abr. 2001 (separata).

10 FERREIRA, *op. cit.* p. 210.

11 GOMES, Flávio Luiz. *Crimes informáticos.* Disponível em: <www.direitocriminal.com.br>. Acesso em 26 nov. 2000.

12 FERREIRA, *op. cit.* p. 214 – 215.

13 ROSSINI, Augusto Eduardo de Souza. *Brevíssimas considerações sobre delitos informáticos.* São Paulo: ESMP, jul. 2002. p. 140 (Caderno Jurídico, ano 02, n. 04).

14 Idem. p. 140-141.

15 Idem. p. 180-210.

16 Art. 2º, inc. IX, Lei n. 1.521/1951.

17 LEVENE, Ricardo; CHIARAVALLOTI, Alicia. *Delitos informáticos. VI Congresso Iberoamericano de Derecho e Informática*, Montevideo. Mayo, 1988. Anais. Montevideo: Ponencias, 1998. p. 123 – 146. 125 p.

18 Idem, p. 125. Os autores citam María de La Luz Lima, sem mencionar sua referência bibliográfica.

19 LEVENE, Ricardo; CHIARAVALLOTI, Alícia. *op. cit.* p. 129 - 130.

20 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente*. Disponível em: <http://www.onu.org/>. Acesso em 17 out. 2002.

21 CARRASCOSA LÓPEZ, Valentin. La regulación jurídica del fenómeno informático. *Mérida: Revista Informática y Derecho*, v. 19/22, p. 33-55, 1998.

22 LEY ORGÁNICA 11/1999, de 30 de abril. Disponível em <http://noticias.juridicas.com/base_datos/penal/1011-1999.html>. Acesso em 26 mar. 2003.

23 TÉLLES VALDÉS, Julio. Terrorismo por computadora. *Mérida: Revista Informática y Derecho*, v. 1, p. 177-183, 1992.

24 Delitos preterdolosos ou preterintencionais são aqueles praticados com dolo no antecedente e culpa no conseqüente, de maneira que o resultado final do crime tenha resultado culposo, como, por exemplo, na hipótese de o agente apenas

querer ferir a vítima com um soco, porém emprega uma força tal que esta vem a cair no solo, bater a cabeça e morre em decorrência das lesões experimentadas.

BIBLIOGRAFIA COMPLEMENTAR

GUIMARÃES, José Augusto Chaves. A ética na formação do bibliotecário: uma reflexão a partir da realidade brasileira. *Information*, Montevideo, n. 2, 1997, p. 96-104.

ABSTRACT

The authors adduce that the reflection concerning the ethical dimension that is inserted in the new informational spaces and supports brought to the information professional's reality requires its displacement from the traditional approach of the internet as an important and valuable space of information availability in order to discuss, in a wider view, the restraints of juridical order to which the inadvertent use of this space can lead.

So, they stress the concepts and the types of crimes committed "with" and "against" the computer, by concluding that the crimes of informatics have to be a social worry and that they lack of typifying in our legal system.

The authors point to the need of an ethical reflection, from the side of the information professionals, so that they could contribute, in a legitimate way, to the access and to the retrieval of information in order that they can be made according to the established juridical framework, acting not only as mere information deliveries, but also as valuable colaborators of the juridical trials which aim to guarantee such rights.

KEYWORDS - Informatics – crime; internet; professional ethics; information.

Mário Furlaneto Neto é delegado de Polícia Adjunto da Delegacia de Investigações sobre Entorpecentes de Marília - SP.
José Augusto Chaves Guimarães é livre-docente em Análise Documentária pela UNESP. Docente do programa de pós-graduação em Ciência da Informação da UNESP – Marília - SP.