Bem Jurídico e os Crimes de Computador

Paulo Marco FERREIRA LIMA*

• RESUMO: Cuida o presente artigo dos bens jurídicos dos crimes praticados por computador e sua recepção pelo sistema penal brasileiro. Aponta necessidade de eventuais alterações legislativas no Código Penal e a criação de novos delitos em legislação especial.

• PALAVRAS-CHAVE: Bem jurídico. Crimes de computador. Internet. Segurança computacional. Alterações legislativas. Fraude eletrônica.

Introdução

O computador tem por *função essencial a concentração e operação* de *informações*, o que traz perigosa assimilação ao nosso modo de vida.

As sociedades ocidentais passam atualmente por uma segunda revolução industrial, substituindo o trabalho das mentes humanas pelo das máquinas computadorizadas.

Ao contrário da primeira, que substituiu o trabalho físico dos operários por máquinas mecânicas, a segunda tem nos computadores sua importância justamente por sua capacidade de imitar, ou tentar imitar o pensar.

É claro que "Era da Informação" não traz somente vantagens, a segurança das informações armazenadas nos sistemas computadorizados ganha gigantesca importância quando no mundo todo as instituições financeiras passam a fazer toda espécie de transações monetárias com uso de computadores (ULRICH, 1992).

O simples *uso de cartões de crédito*, com *arquivamento e processamento de dados eletrônicos*, prática *rotineira* das *instituições financeiras* que operam com essa figura, *pode demonstrar*, pelo exame dos gastos de um associado, muito da esfera de sua *vida privada*, revelando-se aspectos atinentes às suas relações de consumo (*o que compra e em qual quantidade*), *que lugares freqüenta* para compras, hospedagem, refeições, viagens etc..

Assim, ocorreu aumento significativo dos delitos relacionados com o processamento de dados nas Américas, Europa Ocidental, Austrália, Japão, e mesmo em países do antigo bloco socialista e no BRASIL.

Tais crimes não apresentam perigo tão-somente para as empresas privadas, mas também para toda a economia de um país e sua sociedade, e isso levou os países a celebrarem convênios nacionais e internacionais para o combate dos crimes cometidos por intermédio do uso de computadores (ibidem, p. 67).

De outro lado, o direito penal tem seu fundamento nas relações humanas e assim ele acaba sempre em uma eterna caminhada de evolução e de adaptação às novas realidades dessas relações.

A tecnologia muda o homem e muda o direito, *não* exatamente no mesmo *compasso*, provocando muitas vezes *surpresa* e *perplexidade* aos feitores e mantenedores do direito.

Essa nova *intensificação* do *relacionamento humano pela Internet* e a *produção em série dos computadores*, além da *expansão do comércio eletrônico* e das *relações financeiras e bancárias*, provoca o uso indiscriminado e quase mundial dessa tecnologia, favorecendo em todos os aspectos novas relações e modificando as antigas, *trazendo também, por óbvio, novas condutas ilícitas*.

Esses crimes praticados com o emprego dos computadores, a atuação desses novos agentes criminosos (denominados por alguns como *hackers*), restam a *desafiar* o *Estado*, podendo *ofender* de for-

* Promotor de Justiça da Capital. Mestre em Direito Penal pela Faculdade de Direito da Universidade de São Paulo e doutorando pela mesma instituição.

ma indistinta desde *instituições financeiras* até *militares* e, em que pesem *parecer* estarem presentes de forma *incipiente na realidade brasileira*, são a maior *frente de batalha* a ser enfrentada pelos doutrinadores brasileiros.

Surgem questões atinentes à tipicidade, aos novos agentes delituosos e suas diversas condutas, *local do delito*, determinação de autoria, *perícias* documentais etc.

Há uma *infinidade de delitos* que pode ser *praticada com o uso de computadores* e da telemática, além dos *mais óbvios*, como a subtração, e aqueles ligados à *corrupção de menores e pedofilia*, até mesmo exemplo relembrado pela doutrina de que a *manipulação de dados eletrônicos de uma Unidade de Terapia Intensiva* de um hospital possa levar à prática de homicídio[1] ou, ainda, que a manipulação de computadores de um *laboratório militar* possa levar à disseminação de *armamento biológico* e a um possível genocídio.

O *Direito Penal* deve preservar o denominado Princípio da Legalidade, ou também chamado Princípio da Reserva Legal, exposto no art. 5º, inciso XXXIX, da Constituição Federal (CF), segundo o qual "*não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*".

Há perigosa adaptação dos princípios constitucionais.

A descrição há de ser específica e individualizada do comportamento criminoso, sob pena de não trazer uma *garantia real* e efetiva. Não há como se conceber uma lei excessivamente genérica em matéria penal.

A Internet não pode ser entendida como uma "terra sem lei", uma vez considerado que as operações ali efetivadas sempre têm como fundamento relações entre seres humanos, obrigatoriamente regidas pelos princípios gerais do direito.

Desnecessária a *criação de um novo universo jurídico*; o ordenamento jurídico atual é suficiente para a *recepção* dessa nova realidade.[2]

Vários foram os momentos na história do direito penal em que a *tecnologia trouxe evoluções e reviravoltas* nessa ciência.

Foi assim com a criação e difusão de todas as tecnologias inovadoras, como o *automóvel*, o *cartão de crédito*, os computadores e mesmo a *Internet*.

Com relação aos bens jurídicos que podem ser afetados com os delitos informáticos, conclui-se que há dois grandes grupos:

- utilização dos meios computadorizados para a prática de infrações penais comuns;
- utilização da informática com o intuito de atingir bens novos que recai sobre objetos informáticos propriamente ditos (hardwares, programas, dados, documentos eletrônicos etc.).

Não pode ser desprezado pelo Direito Penal que os dados eletrônicos, matéria-prima para as operações computacionais, são bens materiais hoje importantíssimos.

Em que pese a existência da chamada "Lei do Software" (Lei Federal nº 9.609, de 19 de fevereiro de 1998), muito há que se caminhar no sentido de um sistema jurídico protetor de dados eletrônicos e sistemas informáticos.

Não há, ainda, uma figura típica para reprimir as condutas criminosas cometidas por meio de computadores ou contra seus dados e sistemas.

As normas existentes em nosso ordenamento jurídico não protegem de forma plena, por exemplo, os delitos contra a honra cometidos por meios informáticos ou a violação de correspondência eletrônica.

[1] Greco Filho (*Boletim IBCCRIM*, ano 8, n. 95, out. 2000), referindo-se ao homicídio praticado por um *hacker* que invadiu em 1994 um hospital em Liverpool, na Inglaterra, e alterou o medicamento de vários pacientes, provocando a morte de uma menina de nove anos (cf. publicação da revista *Der Spiegel*, n. 94, p. 243, 28 fev. 1994).

[2] Nesse sentido, ver Greco Filho (op. cit.). "A Internet não passa de mais uma pequena faceta da criatividade do espírito humano e como tal deve ser tratada pelo Direito, especialmente o Penal. Evoluir, sim, mas sem querer 'correr atrás', sem se precipitar e, desde logo, afastando a errônea idéia de que a ordem jurídica desconhece ou não está apta a disciplinar o novo aspecto da realidade. E pode fazê-lo no maior número de aspectos, independentemente de qualquer modificação."

Há necessidade de tipificação de condutas ilícitas efetivadas pelo meio informático que vão do acesso não-autorizado a computadores, passando pela falsificação de documentos eletrônicos, até as fraudes eletrônicas.

Outros bens de igual relevância que se encontram sobre intenso ataque dizem respeito à garantia constitucional da inviolabilidade da intimidade e da vida privada, consagrada no art. 5º, inciso X, da Carta Magna, valor jurídico em muito ofendido com a tecnologia informática.

Assim é que ações ilícitas cometidas contra tais bens de cunho informático são objetos de projetos legislativos que visam à tipificação de condutas, seguindo modelos legislativos de outros países que, no mais das vezes, apontam crimes de sabotagem informática, fraude eletrônica, cópia ilegal e intrusão informática.

Faço aqui também apenas a rotineira menção de que o uso de tecnologia de computação levou a uma maior fragilidade do sigilo das informações. Primeiro porque os dados pessoais que anteriormente eram restritos a um número determinado de pessoas em registros físicos se encontram hoje, muitas vezes, à disposição de milhões de pessoas no mundo que tenham uma conexão da Internet e um pouco de torpeza e habilidade para obtê-los; segundo porque, atualmente, na chamada "era da informação", o tráfego de dados é por demais intensificado, fazendo que essa célere e constante troca de informações exponha ainda mais a vida privada e o sigilo de informações pessoais relevantes.

É evidente que as adulterações de dados eletrônicos põem em risco a necessária confiabilidade das comunicações e dos negócios eletrônicos. Porém, o momento é propício ao incremento de medidas penais que produzam efeitos em todos os campos afetados pela informática, trazendo, com isso, normas que de forma efetiva atendam à necessária proteção a todos os bens jurídicos ofendidos por intermédio de computadores.

Crimes de computador e o Código Penal

Assim, os *crimes de informática* encontram no Código Penal brasileiro várias possibilidades de repressão penal, variando a sua tipificação conforme o bem jurídico que o agente pretenda atingir.

Existem diversos crimes no Código Penal que, em tese, poderiam ser praticados por intermédio de computadores, entre os quais se encontram:

- art. 171, *caput*, estelionato;
- art. 172, expedição de duplicata simulada;
- crimes contra o privilégio de invenção (arts. 187 a 191, revogados pela Lei nº 9.279/96);
- falsificação de documento público (art. 297) e particular (art. 298);
- falsidade ideológica (art. 299);
- crimes contra a inviolabilidade da correspondência (art.151);
- correspondência comercial (art. 152);
- divulgação de segredo (art. 153), ou violação de segredo profissional (art. 154).

Os dispositivos penais supracitados devem mesmo ser aplicados às condutas praticadas pelo meio informático que constituam crimes comuns, contudo, em alguns casos, são indispensáveis alterações, por exemplo, criando qualificadoras quando o uso de um sistema informatizado for ferramenta simplificadora da prática criminosa.

Conclusões

O progresso na tecnologia da comunicação, mormente com o surgimento da Internet, trouxe novas relações jurídicas, com novos conflitos e uma série infindável de novas controvérsias.

No mundo todo, o Direito vem mudando para conseguir exercer com a necessária rapidez e eficiência o controle social dessas inovações, modificando as estruturas legislativas para lidar de forma adequada quanto às novas e polêmicas questões.

O Brasil necessita adaptar a legislação penal para coibir essas novas lesões e ameaças às liberdades individuais e ao interesse público. Toda a legislação, e em especial a lei penal moderna, deve atentar para a proteção dos bens jurídicos informáticos e de outros que possam ser ofendidos por meio do uso de computadores.

Nessa esteira de pensamento, devem os operadores do direito buscar a redefinição de alguns

conceitos como o de documento para fins penais e o de crime de falsidade documental, entre outros tantos.

Com o intuito de concluir, afirmamos ser dispensável a criação de um novo ordenamento jurídico para recepcionar essa nova prática criminosa que visa atingir, de forma precípua, o sigilo e a integridade de dados eletrônicos, à qual denominamos *crimes de informática* ou *crimes de computador*.

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

Sugere-se, para o combate dessa nova criminalidade, a adaptação de leis e conceitos, visando à proteção dos bens jurídicos a serem tutelados pelo Direito Penal Informático.

Muitos dos chamados crimes de computador são, na verdade, os crimes comuns cometidos com o auxílio de um computador; porém, estamos também diante de novas condutas não tipificadas que ofendem uma série de bens jurídicos penalmente tutelados, sem que sejam esses objeto de uma figura típica específica.

As ações criminosas praticadas com essa nova tecnologia de informação, dirigidas contra a liberdade individual, contra o direito à intimidade ou ao sigilo das comunicações entre outras, ainda se encontram sem a devida repressão jurídico-penal.

As lacunas permanecem também em face da ausência de condutas consideradas antijurídicas e típicas atinentes às fraudes cometidas com a manipulação de dados e programas computadorizados, ou seja, as fraudes cometidas com a utilização abusiva de computadores por meio de adulterações em documentos eletrônicos, provocando danos financeiros. Tais ações se encontram em perigosa zona nebulosa de repressão penal.

A "era da informática" veio expor diversos bens de forma mais ampla e abrupta, sendo certo afirmar que os dados constantes em um documento eletrônico encontram-se mais desprotegidos hoje do que quando restavam somente em um fino pedaço de papel.

Podemos assim distinguir duas categorias de crimes informáticos:

- condutas delituosas perpetradas contra um sistema de informática, sejam quais forem as motivações do agente;
- crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática.

No Brasil, em que pese a existência de legislação disciplinando crimes na área de informática desde a Lei nº 7.646/87 (revogada pela Lei nº 9.609, de 19 de fevereiro de 1998), muito ainda há que ser feito no sentido de criar um sistema jurídico protetor de dados eletrônicos e sistemas informáticos.

Não há, ainda, embora existam diversos projetos legislativos em tramitação, figuras típicas eficientes para reprimir todas as condutas criminosas cometidas por meio de computadores ou contra seus dados e sistemas.

Assim, seja no território brasileiro,seja em outros lugares do mundo, ponderando quanto aos aspectos econômicos e financeiros de tais crimes ou, ainda, tendo em vista todos aqueles que utilizam essa tecnologia de informação – como instituições financeiras ou o próprio Governo Federal em seus diversos órgãos –, intensificam-se os investimentos em desenvolver medidas legislativas de proteção aos dados computadorizados.[3]

[3] Por exemplo, salientem-se as diversas medidas que vêm sendo tomadas com relação ao envio ilegal de e-mails. Trazemos aqui em destaque notícias veiculadas pela mídia: "Brasil está em quarto lugar no envio de spam – sexta-feira, 23 de setembro de 2005 – 14h24 – SÃO PAULO – O Brasil é o quarto colocado entre os países que mais distribuem spam, segundo um relatório da IronPort sobre vírus e e-mails indesejados que circularam pela web no mês de agosto. A posição é a mesma ocupada no mês de julho. A boa notícia é que houve uma leve queda de 3% no volume de spam distribuídos no país em comparação com os dados de julho. A média diária de envio de e-mails indesejados em agosto foi de 12,5 bilhões de mensagens contra 12,8 bilhões no mês passado. Essas mensagens responderam por 69% do tráfego de e-mail na web. O relatório revela que mais de 72% dos spams foram enviados por PCs zumbis. No mês de agosto, 8,9 bilhões de

Agora que a informação se separou de seu suporte material cartáceo, fazendo-se eletrônica, converteu-se em mercadoria armazenável, comercializável, manipulável e avaliável em termos patrimoniais, merecedora de proteção jurídica como qualquer outra mercadoria.

Tais crimes ocorrem no solo brasileiro todos os dias, tendo sido as questões resolvidas mediante uma "pseudo-adaptação típica", proibida pela lei penal e constitucional, mas que se vê construída pelas rotinas judiciárias. Desse modo, essas ações criminosas ora são apontadas como estelionato, ora como furto mediante fraude, desprezando-se os elementos essenciais desses crimes que apontam a mencionada e indispensável relação entre seres humanos para a configuração de ambos os crimes.

O ordenamento jurídico penal brasileiro é deficiente em oferecer resposta aceitável para a perfeita solução quanto às condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet e que não encontram adequação típica no estreito rol de delitos novos existentes no Código Penal e nas parcas leis especiais brasileiras que tratam da matéria.

Não cremos, ainda, aceitável o esforço interpretativo atual que tenta adequar as fraudes e outros crimes à nossa legislação penal, evidenciando-se a atipicidade dessas condutas.

Além do patrimônio, a veracidade e a confiabilidade da informação eletrônica, absolutamente necessárias para a manutenção da confiança que os usuários dos meios eletrônicos e da Internet – uma enorme parte da população mundial – devem depositar no funcionamento de todo o sistema, são o bem jurídico merecedor de preservação penal.

Por fim, fato é que toda a legislação brasileira, em especial a de natureza penal, necessita de uma real adaptação à nova tecnologia informática. Novas normas deverão ser criadas para a melhor prevenção e repressão de ações criminosas outrora impossíveis de imaginar com a realidade tecnológica de então.[4]

FERREIRA LIMA, P. M. Property and computer crimes. *Rev. Justitia* (*São Paulo*), v. 197, p. 381-385, jul./dez. 2007.

• ABSTRACT: Watches this article the legal values of crimes committed by computer and its receipt by the Brazilian penal system. Points need for any legislative amendments in the Penal Code and the creation of new crimes in special legislation.

• KEYWORDS: Property. Computer crimes. Internet. Information technology safety. Legislative changes. Electronic fraud.

Referências bibliográficas

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a Internet. *Boletim IBCCRIM*, ano 8, n. 95, out. 2000. (Edição especial).

SIEBER, Ulrich. *Documentación para una aproximación al delito informático.* Tradução para o espanhol de Ujala Joshi Jubert, professora de Direito Penal da Universidade de Barcelona. Barcelona: PPU, 1992. Título III, cap. 2, p. 66.

PCs foram utilizados em todo o mundo como zumbis. O líder do ranking entre os países que mais enviam spam são os Estados Unidos. Em segundo lugar está a China, seguida pela Coréia do Sul – *1/03/2003 13h18 – UOL barra 7 milhões de spams por dia* – Desde janeiro, os assinantes do UOL vêm recebendo cada vez menos e-mails não-solicitados (spam). O maior provedor de Internet do país implantou em seus servidores de e-mail um conjunto de filtros capaz de barrar grande quantidade de spam, os e-mails de propaganda não-solicitada que ocupam inutilmente espaço na caixa postal do público, tomando tempo para triagem e limpeza de mensagens. Com a implantação do sistema, 47% dos 15 milhões de e-mails que passam diariamente pelos servidores do UOL são barrados, por serem considerados spam. *Sexta-feira, 28 de fevereiro de 2003 – 09h01 Renata Mesquita, do Plantão INFO* – França proíbe o spam – O spam está banido da França a partir desta semana. Com unanimidade, os deputados da Assembléia Nacional aprovaram a lei que proíbe o envio de mensagens comerciais não-solicitadas. Segundo o site Europamedia.net, além da nova lei foram aprovadas emendas que visam aumentar a confiança na economia digital e o combate ao cibercrime. Algumas campanhas de marketing direto (como newsletters de lojas virtuais) continuam liberadas, desde que o internauta tenha se registrado no serviço ou dado seu consentimento prévio.

[4] É bom lembrar que a Parte Especial do Código Penal brasileiro foi elaborada em 1940.