CRIMES PRATICADOS PELO COMPUTADOR. DIFICULDADE NA APURAÇÃO DOS FATOS

Antonio Scarance Fernandes[*]

SUMÁRIO: 1. Introdução. 2. Os crimes praticados por computador. 3. A legislação. O enquadramento na legislação em vigor. 4. Aspectos processuais.

1. Introdução

O avanço da tecnologia trouxe os computadores. Passaram a fazer parte da vida moderna, estando nas residências, nos escritórios, nas empresas, nos órgãos públicos, servindo para os mais variados misteres: o estudo, a pesquisa, a contabilidade, a redação, os serviços bancários. Com eles, sobreveio a formação de espessa e extensa rede de comunicação que liga um computador a outro, sem medir qualquer distância[1]. Só se fala, atualmente, na "navegação" pela Internet. Representou, enfim, a informática uma nova revolução, segundo Miguel Angel Torres Morato, unindo dois elementos fundamentais de nossa civilização: a informação e a comunicação. A informação, diz ele, é o conteúdo da mensagem, são os dados processados. A comunicação é o movimento e transmissão da informação[2].

Mas, com esse avanço, surgiram também problemas graves ligados ao uso do computador.

Um dos primeiros foi a "pirataria". Era fácil, a partir de um disquete criar outros e, assim, os programas passaram a ser copiados. As empresas produtoras dos programas viram-se na contingência de, a cada ano, alterá-los, aperfeiçoá-los, a fim de mantê-los atraentes. Foram feitos movimentos no sentido de inibir as cópias dos programas, com intensa divulgação dos crimes que estariam sendo cometidos.

---

* Professor de Direito Processual Penal da Universidade de São Paulo e professor convidado do Curso de Mestrado em Direito da Universidade Estadual de Maringá.

1 As redes de computadores são "sistemas de computadores interligados por equipamentos de telecomunicação" (Otto Banho Licks e João Marcelo de Araújo Júnior, Aspectos penais dos crimes de informática no Brasil, p. 93). Os autores exemplificam com várias redes: Access, Westlaw, Nexis, Lexis, EFT, Switf, Bitnet, Arpanet, UUCP, Internet, Dec Enet, Videotext, Genie, Compuserve, Reuters. A mais divulgada é a Internet.

2 Miguel Angel Torres Morato, La Prueba Ilícita Penal, p. 275.

Nesse contexto, aparece o devastador "vírus"[3], ao que parece, inicialmente, para destruir programas produzidos por cópias "piratas", mas depois disseminando-se em grande número e extensa variedade, a atacar os computadores de forma indiscriminada, danificando programas e dados informativos. Havia, de início, clara tentativa de forçar os consumidores a adquirir programas originais. A proliferação, contudo, principalmente em face do uso da "internet", desses "vírus", tornou todo programa e todo computador vulnerável, havendo necessidade de constante vigília e de freqüente atualização de programas "antivírus'.

Outro grave problema foi a invasão dos computadores, não mais pelos "vírus", mas por pessoas que, movidas por curiosidade ou realmente mal intencionadas, passaram a ingressar nos computadores alheios. De início, não se preocupou com a segurança dos registros armazenados e o homem confiava no seu computador, silencioso, mudo, criado servil que o auxiliava na sua faina diária. Todavia, com a comunicação entre os aparelhos, principalmente através de redes, a intimidade dos registros passa a ser objeto de desnudamento. Difícil evitar, com plena certeza, que o computador, quando ligado a outro, não seja atacado. Diz Maria Helena Junqueira Reis que a "segurança total dos computadores ainda é um mito. Os muitos estudos na área são recentes. Segundo *Fantinari*, foi só a partir de 1984, nos EUA, é que se começou a *fortalecer* os procedimentos para garantir a invulnerabilidade dos computadores. É evidente que os computadores não se encontram completamente desprotegidos, mas o que vimos até agora prova que existem *fraquezas* nos sistemas[4]. A segurança na Internet passa a exigir que as mensagens sejam criptografadas[5], mas também aí não segurança total, havendo registros de desvendamento de mensagens criptografadas[6].

---

[3] O vírus consiste em "programa, ou *software*, especialmente elaborado para, dissimuladamente, criar processos de infecção de computadores para computadores, capazes de inutilizar dados armazenados ou alterar o normal funcionamento dos programas preexistentes no equipamento do computador afetado" (Fernando Galvão da Rocha, Criminalidade do computador, p. 530). Maria Helena Junqueira Reis, com base em estudos de Ricardo Cidale, Fernando Mismetti e outros, Computer crimes, p. 34-5, classifica os "vírus" em inócuos, alteradores, catastróficos e genéricos. Refere, assim, desde aqueles que "não causam perturbação ao sistema", até os altamente contagiosos (genéricos), e que 'se escondem no meio, começo e fim dos programas, e, geralmente, não interferem com o processo de execução normal dos *softwares*. Parecem invisíveis. Em determinado momento, em resposta a um sinal esperado, são ativados e começam a modificar ou a destruir arquivos". Todos causam graves problemas. Os que denomina de alteradores, mudam dados e, assim, se demorarem a ser descobertos, podem causar danos irreparáveis. Os "vírus catastróficos" são os que "apagam arquivos de sistema, corrompem registros e, em alguns casos, destróem ou inutilizam todas as informações no disco rígido e em outros dispositivos conectados ao sistema."

[4] Maria Helena Junqueira Reis, Computer crimes, p. 35. Citou João Marcos Fantinatti, Segurança em informática, São Paulo, McGraw - Hill, 1988.

[5] O uso da criptografia tem sido apontado como o mecanismo mais eficaz, por enquanto, para que o usuário garanta sua privacidade, conforme noticiário da página de informática do Jornal da Tarde de 17 de junho de 1999. A criptografia, conforme Folha de São Paulo, 22.11.98, é "a técnica que permite tornar uma mensagem incompreensível para quem não possua os instrumentos corretos para decifrá-la. Nos bancos, é o programa que embaralha as informações (número da conta ou

Os jornais noticiaram amplamente que grupo de "hackers"[7] invadiram os "sites" dos Três Poderes (Palácio do Planalto, Supremo Tribunal Federal e Câmara dos Deputados), no mês de junho de 1999, inserindo nessas páginas textos de protesto contra o governo, a privatização de estatais e o Fundo Monetário Internacional. Invasões anteriores já haviam acontecido, entre nós, como a ocorrida no site da Confederação Brasileira de Futebol em julho de 1998. Nos Estados Unidos tem havido invasão de muitos "sites", chegando a ocorrer até mesmo nos sites da FBI e do Senado[8].

Assim, as maravilhosas máquinas eram vulneráveis e serviam também para propósitos desonestos, inclusive para a prática de crimes. Pouco a pouco foram despontando os ilícitos cometidos: a invasão dos dados alheios, o desvio de dinheiro de uma conta bancária para outra, a transmissão de cenas eróticas e, até mesmo, com utilização de crianças (pedofilia).

A vulnerabilidade dos dados do computador traz, ainda, outro reflexo importantíssimo para a sociedade. Como o computador passou a fazer parte essencial da vida cotidiana, o conhecimento de seu conteúdo pode representar grave invasão da privacidade, permitindo que o acesso aos dados e o cruzamento com outros revele o perfil de determinada pessoa, indicando suas idéias políticas, sua convicção religiosa, suas enfermidades, seu grau de instrução, seu trabalho, sua posição econômica. A pessoa que acessou a Internet, ao voltar para uma homepage é, se não tiver dispositivos especiais de segurança, reconhecida pelo sistema, em virtude da atuação dos "cookies". Estes constituem "pequenos arquivos que ficam gravados no disco rígido e que têm como objetivo informar ao servidor de uma página Web que você está visitando o site novamente. A identificação é feita por meio de uma combinação de números e letras, não com nome ou outros dados pessoais"[9].

Por isso mesmo, constou da Constituição da Espanha que: "A lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos". Surge daí a necessidade de haver controle sobre quem pode ter acesso aos dados de um computador e, ainda, manifesta-se um novo direito o de a pessoa poder alterar os dados incorretos ou inverídicos a seu respeito pelo uso do "habeas data"[10]. Esse direito, protegido pelo

---

senha), impedindo que ela seja interceptada por um estranho. Funciona como se fosse o segredo de uma fechadura. Só quem tem a chave pode abri-la".

6 Maria Helena Junqueira Reis, Computer crimes, p. 54.

7 Os "hackers" são pessoas conhecedoras de informática e que usam seu conhecimento para ingressar nos sistemas e programas de computador. Quando têm intenção de praticar fatos ilícitos são conhecidos por "crackers".

8 Folha de São Paulo, 19 de junho de 1999, 1-7.

9 Jornal de Informática do Jornal da Tarde, 17 de junho de 1999, p. 3D.

10 Ver sobre essa preocupação no tocante à privacidade em virtude do computador Miguel Angel Torres Morato, La Prueba Ilícita Penal, p. 275-282, com especial destaque à legislação espanhola. Refere, ainda, no plano internacional a Convenção do Conselho da Europa de 18 de janeiro de 1981

"habeas data", é denominado pela doutrina direito à liberdade informática ou à autodeterminação informática, sendo conceituado como o "direito de controlar (conhecer, corrigir, apagar ou complementar) os dados pessoais inscritos em um programa eletrônico"[11].

Mais grave. Os crimes por computadores não têm fronteira. São marcados pela universalidade. Alguém, dentro do país, pode cometer a infração em região distante. Pode praticar a infração em computador de outro país. Não há limite. A distância não importa para ele. Além disso, facilita o anonimato.

Com tudo isso, passa o tema da "criminalidade do computador" a ser objeto de preocupação e de debate. São muito altos os prejuízos advindos dessas práticas.[12]

Nesse contexto, surge o direito informático[13] e, como um desses ramos, o direito criminal informático[14], cujo âmbito de preocupação são os crimes cometidos por computador.

2. Os crimes praticados por computador

A dificuldade no exame do tema inicia-se com a própria conceituação e denominação da nova espécie de crime produzido por computador. Fala-se em "crime informático", "crime por computador", "crime da informática", "delito informático', "abuso de informática", "abuso de computador", "crime de computação", "delinqüência informática", "fraude informática". São denominações

para a proteção da pessoas em relação ao tratamento automatizado dos dados de caráter pessoal. Ver ainda sobre o habeas data Pérez Luño, Manual de Informática y derecho, p.44 e seguintes.

[11] Pérez Luño, Manual de Informática y derecho, p.43.

[12] Fala Fernando Galvão da Rocha (Criminalidade do computador, p. 523) das elevadas dimensões econômicas que envolve a informática. Assim, em "1994 foram fabricados em todo o mundo 49 milhões de computadores pessoais"; "nos Estados Unidos, o mercado de informática movimenta 7,7 milhões de dólares com equipamentos e 4 milhões de dólares em programas"; "no Brasil, estima-se que o mercado de informática já movimente entre 5 a 8 bilhões de dólares". Salienta Valdir Sznick (O delito e o computador, p. 48) que no ano de 1980, nos Estados Unidos, calculava-se que o mau uso do computador havia causado "um prejuízo da ordem de 400 milhões de dólares", sendo estimado "que apenas 20 % dos casos de criminalidade de informática tenham sido levados a julgamento e, desses, apenas 3 % resultaram em condenações". Refere Maria Helena Junqueira Reis, Computer crimes, p. 14, que, em virtude de crimes por computador, na Suíça, as Companhias Seguradoras, perdem anualmente 2,86 milhões de dólares'; na França, a soma resultante destes delitos atingiu, no ano de 1984, a soma de 700 milhões de francos. Também no Brasil, mencionam-se elevados prejuízos resultantes de "vírus" malignos (p. 15). A tudo se acrescente que a grande maioria das infrações praticadas por computadores não são noticiadas, porque as empresas atingidas não as divulgam com receio de perda de credibilidade junto a seus clientes.

[13] Define-se o direito informático como o "conjunto de normas, princípios e instruções que regulam as relações emergentes da atividade informática" (Altmark, citado por Maria Helena Junqueira Reis, Computer crimes, p. p. 14). Trata-se de matéria multidisciplinar que abrange vários ramos do direito tradicional. Sobre os elementos conceitos, objeto e metodologia do direito informático ver Pérez Luño, Manual de Informática y derecho, p. 18-21.

[14] O direito informático abrange várias disciplinas do direito tradicional: civil, comercial, penal, trabalhista. É, essencialmente, interdisciplinar.

que, com maior ou menor amplitude, apresentam-se semelhantes. Podem todas ser utilizadas, dependendo do enfoque dado ao tema. Denominação bastante significativa e muito utilizada é a expressão: crime informático.

O que seria esse crime informático?

Não há uniformidade na sua definição.

Apresenta conceito bastante amplo Gustavo Arocena. Entende, na linha do pensamento de outros autores (Carlos Maria Correa, Tiedeman) que representam crimes informáticos todas as formas delitivas que utilizam os sistemas informáticos como meio comissivo ou que o têm, em parte ou totalmente, como seu objeto. Em outras palavras, qualquer ação em que o computador seja o instrumento ou o objeto do delito. Mais genericamente, ainda, qualquer delito ligado ao tratamento automático de dados. Fala, contudo, em delitos informáticos próprios e impróprios, referindo-se aos primeiros como aqueles que só podem ser concebidos em face de um sistema informático e aos segundos como os que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo[15].

Para Donn Parker, citado por Maria Helena Junqueira Reis, "Abuso de computador é ... qualquer incidente ligado à tecnologia do computador, no qual uma vítima sofreu, ou poderia ter sofrido um prejuízo, e um agente teve, ou poderia ter tido, vantagens[16]. Trata-se de noção ampla mas que limita o crime informático aos crimes que causem prejuízo patrimonial.

Já Otto Banho Licks e João Marcelo de Araújo Júnior restringem a noção de crime informático. Entendem que a "preocupação do Direito Criminal de Informática ... deve-se, fundamentalmente, à proteção dos seus componentes imateriais ou intangíveis, ou seja, o *software* e os "dados" ... e, principalmente, do que chamam de "recurso disponível, proveniente da utilização dos sistemas de computadores em redes de computadores". Não incluem a proteção da propriedade intelectual do Direito contra a "pirataria" ou a contrafação, já reguladas pela tutela penal. Limitem, portanto, o âmbito dos crimes informáticos, definindo-os, primeiramente, através do bem jurídico. "Crime de informática é a conduta que atenta, imediatamente, contra o estado natural dos dados e recursos oferecidos por um sistema de processamento, armazenagem ou transmissão de dados, seja em sua forma, apenas compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenamento de dados, seja na sua forma compreensível pelo homem". "Em segundo lugar, o crime de informática é aquele que atentando contra estes dados, o faz de forma também compreensível por um sistema de tratamento, transmissão ou armazenamento de dados". A partir daí

---

[15] Gustavo A. Arocena, De los delitos Informaticos, Revista de La Facultad de Derecho y Ciencias Sociales da Universidad Nacional de Córdoba, p. 50-54.

[16] Maria Helena Junqueira Reis, Computer crimes, p. 25.

diferenciam os crimes de informática de outros, comuns, praticados por meio do computador[17].

Como dito, importa muito o enfoque pretendido. Para o penalista, preocupado em estudar os tipos novos surgidos com o uso do computador e que dele necessitam para existirem e, ainda, os tipos antes existentes e com vida própria, independente do computador, a denominação "delito informático" é aconselhável, com a conseqüente separação do delito informático em "puro" (o delito da primeira espécie) e delito informático "impuro" (o delito da segunda espécie). Mas, para quem almeja examinar, de forma mais ampla, tais crimes, principalmente no que se refere à sua descoberta e à sua persecução, a denominação "crimes praticados por computador" ou "crimes por computador" se apresenta bastante ajustada. Interessa, aí, o estudo de qualquer tipo de crime informático, puro ou impuro, desde que cometido pelo computador, aproveitando-se das facilidades decorrentes do seu uso e, principalmente, do anonimato por ele assegurado.

Outro aspecto importante é o exame das diversas formas de serem delimitados e classificados os crimes praticados pelo computador.

Segundo Pérez Luño, o delito informático é examinado segundo tendências diversas. Refere tendências subjetivas, que realçam o agente (hackers, outsiders, insiders), objetivas (fraudes, sabotagem, espionagem, furto de serviços, acesso não autorizado) e funcionais (atentados referentes às fase de entrada - input - ou de saída - output do sistema, sua programação, elaboração, processamento de dados e comunicação telemática)[18].

Na linha subjetiva, Ulrich Sieber leva em conta, na sua classificação, a forma de atuação do autor, indicando, assim, os seguintes crimes: a) fraude por manipulação de um computador contra um sistema de processamento de dados; b) espionagem informática e furto de software; c) sabotagem informática; d) furto de tempo; e) acesso não autorizado a sistemas; f) ofensas tradicionais. Nestes tipos procura enquadrar as mais diversas condutas. Assim, a conduta que objetiva atingir dados de contas bancárias para obtenção de vantagem econômica corresponderia à primeira espécie, ou seja, à fraude por manipulação de um computador, que tanto pode introduzir dados falsos ou modificar os registros[19].

Como classificação funcional, tem-se a de C.M. Romeo Casabona: a) manipulação de entrada de dados (input) - introdução de dados falsos no computador, modificação de dados reais, introdução de dados completamente fictícios, omissão de registros de dados: b) manipulação no programa - modificação ou eliminação de alguns passos do programa; introdução de partes novas no programa; c) manipulação na saída de dados (output) - alteração no momento da

---

[17] Otto Banho Licks e João Marcelo de Araújo Júnior, Aspectos penais dos crimes de informática no Brasil, p. 89 e seguintes.

[18] Pérez Luño, Manual de Informática y derecho, p.70-5.

[19] A classificação foi extraída da obra de Maria Helena Junqueira Reis, Computer crimes, p. 29-31.

impressão ou no envio dos dados para outro computador; d) manipulação à distância - alterações nos dados de computadores por outro com o qual se encontra conectado[20].

A maioria tende a utilizar classificações objetivas, com especificação dos tipos de crimes cometidos pelo computador, variando os critérios definidores das espécies. Deste teor é a classificação de Bassiouni, apresentada por João Marcelo de Araújo Júnior em relatório para conferência na Alemanha. Leva em conta o direito violado. Separa, então, os crimes em: crimes contra a privacidade; crimes contra a propriedade individual ou coletiva por meio de fraudes (manipulações, espionagens, pirataria), furto de tempo e sabotagem; contra a segurança nacional ou internacional[21].

Outros também fazem classificações objetivas.

Pérez Luño refere os tipos comuns de crimes por computador. Quanto às fraudes cita a dos "dados enganosos"(data didling), "cavalo de Tróia" (troyan horses), a técnica do salame (salami technique/ rounding down). Em relação às sabotagens, refere as "bombas lógicas" (logic bombs), os vírus informáticos. Refere, como caso de espionagem eletrônica, a "fuga de dados"(data leakage). Sobre o furto de tempo, menciona a "apropriação de informações residuais" (scavenging), "parasitismo informático (piggybacking). Relaciona algumas modalidades de acesso não autorizado: "as portas falsas" (trap doors), "a chave mestra" (superzapping)[22]. Carlo Serra e Marco Strano referem técnicas semelhantes para a prática de crimes por computador: data didling, troian horse, salami techiniques, trap door, trashing, scavenging, logic bomb, time bomb, inpersonation, kacking e cracking, sniffers[23].

Entre nós, Augusto Rossini separa os crimes em face da maneira como é utilizado o computador. Menciona "três tipos de crimes: puro (visa especificamente computadores, como no caso de *hackers*), misto (computador é ferramenta do crime, por exemplo, roubo de informações para invadir bancos) e comum (semelhante ao cometido em outros meios, como páginas de pedofilia)"[24]. Valdir Snick refere as principais técnicas aplicadas no cometimento de crimes por computador: 1. Lata de lixo; 2. Superzapping; 3. Data Didding; 4. Cavalo de Tróia. O sistema que denomina de "lata de lixo" consiste na obtenção dos códigos utilizados no computador através de restos de lançamentos de computadores nas latas de lixo. O "superzapping" configura através da "quebra do programa do computador", paralisando-o e "impedindo que ele realize suas operações normais e, com isso, sendo permitido o acesso ao banco de dados e memória, e, portanto, a todo o sistema". No "data didding" há "troca de cartões, discos e fitas dos

---

[20] A classificação foi referida por Maria Helena Junqueira Reis, Computer crimes, p. 31-2.

[21] A classificação é citada por Maria Helena Junqueira Reis, Computer crimes, p. 32.

[22] Pérez Luño, Manual de Informática y derecho, p. 70-5.

[23] Carlo Serra e Marco Strano, Nuove frontiere della criminalità, Giuffré, p. 37-42.

[24] Folha de São Paulo, 4.8.98, 3-8.

originais, por outros falsos", introduzindo-se novos comandos e com isso, alterada a programação originária, torna-se possível o "acesso ao banco de dados com todos os registros e codificações". Finalmente, o "Cavalo de Tróia" que consiste na "sabotagem de um programa", colocando-se outras instruções em lugar das instruções originais e normais, sem destruir o programa original[25] [26].

Aspecto especial é a criminalidade pela Internet, assim definida por Joshua Eddings: "sociedade de milhares de organizações e redes que trabalham cooperativamente sem um governo ou administração central"[27]. A falta desse governo central, o crescimento da Internet sem nenhum sistema de controle, a possibilidade de manter ou receber informações anonimamente torna difícil a persecução e a punição de delitos dela decorrentes. Diz Maria Helena Junqueira Reis, que a "gama de delitos que podem ser perpetrados pela Internet é quase infinita. A lista inclui o mau uso dos cartões de crédito, ofensas contra a honra, apologia de crimes, como racismo, ou incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de arquivos, programas copiados ilegalmente e até crime eleitoral (propaganda não autorizada por exemplo)". Noticia, nos EUA, processos relacionados com propaganda enganosa, problemas relativos a direito autoral etc.. Refere Fernando Galvão da Rocha as condutas consistentes em interceptar e desviar as informações transmitidas por Internet para equipamento clandestino[28].

3. A legislação. O enquadramento na legislação em vigor

Não há, entre nós, lei que defina e puna os denominados crimes praticados por computador, cujo objetivo seja proteger os dados informatizados. Foram apresentados projetos, ainda não transformados em lei[29].

---

[25] Valdir Sznick, O delito e o computador, p. 50.

[26] Sobre o 'cavalo de Tróia", diz a Folha de São Paulo, 22.11.98, 3-2, que, como "no lendário cavalo de madeira grego esse tipo de programa contém surpresas em seu interior. Hackers costumam usar imagens banais como um jogo, ou anexos de e-mail para camuflar um cavalo de Tróia. Os mais terríveis desses programas são o Back Orifice e o Net Bus. Com o Back Orifice, o seu computador pode ser controlado à distância e sua senha, desvendada. ... " O "hacker" pode ligar o microfone do computador com "o Net Buss e escutar" as conversas nele realizadas.

[27] Joshua Eddings, Como funciona a Internet, citado por Maria Helena Junqueira Reis, Computer crimes, p. 52.

[28] Fernando Galvão da Rocha, Criminalidade do computador, p. 529.

[29] Maria Helena Junqueira Reis, Computer crimes, p. 49-51, relaciona os projetos arquivados e em discussão sobre os crimes de computador no Brasil. O mais antigo é o Projeto de Lei n ° 3.279, de 1976, que dispunha sobre a programação viciada do computador. Depois dele foram apresentados os Projetos de números 96, de 1977; 4.125, de 1989; 579, de 1991; 152, de 1991; 4102, de 1993; 75, de 1989. Fernando Galvão da Rocha, Criminalidade do computador, p. 531-4, examina o Projeto 152, de 1991, de autoria do então senador Maurício Correia que define crimes contra a inviolabilidade de dados e sua comunicação e considera documento o dado constante de sistema eletrônico que, por qualquer razão, tenha relevância nas relações entre pessoas". Mais recentemente, o Ministério da Justiça noticiou que iria enviar projeto de lei sobre crimes cometidos

Discute-se se deve haver legislação específica. A tendência na Europa é a elaboração de leis tendentes a proteger os dados e informações contidos no computador. [30] Para alguns, basta o sistema normativo vigente, no qual seria possível enquadrar todas as condutas delituosas praticadas por computador.[31] Outros entendem ser necessária legislação específica[32] [33]. Esta é a melhor solução. Ainda que a maioria dos crimes possam ser enquadrados no sistema vigorante, há ações que não podem ser nele tipificadas e, ainda, há dificuldade na adequação de outras condutas. O ingresso não autorizado em outro computador, assim como se pune a violação de domicílio, já devia ser punido, o que, contudo, não é possível com os tipos ora encontrados[34]. Por outro lado, a subtração de dados gera interessante discussão sobre a ocorrência de furto, divergindo-se em torno da existência, no caso, de "coisa".

O que existe é lei que protege o *software*, ou seja, "um conjunto organizado de *instruções* em linguagem natural ou codificada, contida em suporte

---

por meio de computador. Segundo informação da Folha de São Paulo (26.3.99, A9) a "intenção é especificar ou tipificar ilegalidades, como o desvio de cartões de crédito, o chamado terrorismo cibernético - quando alguém entra na base de dados de uma empresa para sabotagem - ou o uso indevido da Internet". Pretende o governo que esse assunto seja tratado fora do Código Penal, assim os crimes praticados por computador ficaram fora da reforma do Código Penal projetada. Ver, ainda, sobre os projetos mais importantes Otto Banho Licks e João Marcelo de Araújo Júnior, Aspectos penais dos crimes de informática no Brasil, p. 98-101.

30 Fernando Galvão da Rocha, Criminalidade do computador, p. 528, lembra que na Europa somente a Itália e a Grécia não possuem lei de proteção aos bancos de dados. Na Itália, contudo, segundo Salvatore Ardizzone (A legislação italiana em matéria de *computer crimes.* Entre direito e política criminal, p. 103-125, nos anos de 1992 e 1993 vários textos, por ele analisados, alteraram o panorama existente, passando a punir condutas referentes a crimes de computador. Na Espanha, segundo Miguel Angel Torres Morato, La Prueba Ilícita Penal, p. 279-80, o novo Código Penal, prevê no artigo 197.2. como criminosa a conduta de quem "se apodere, utilize ou modifique, em prejuízo de terceiro, dados reservados de caráter pessoal ou familiar de outro que se achem registrados em fichários ou suportes informáticos, eletrônicos ou telemáticos, ou em qualquer tipo de arquivo registro ou privado" e, ainda, a de quem, sem estar autorizado, "acesse por qualquer meio aos dados" ou quem "os altere ou utilize em prejuízo do titular dos dados ou de um terceiro".

31 Gustavo Arocena, De los delitos informáticos, cita autores que assim se orientam e indica os fundamentos de suas posições (p. 44-6)

32 Assim Fernando Galvão da Rocha, Criminalidade do computador; Valdir Sznick, O delito e o computador; Otto Banho Licks e João Marcelo de Araújo Júnior, Aspectos penais dos crimes de informática no Brasil.

33 Otto Banho Licks e João Marcelo de Araújo Júnior, Aspectos penais dos crimes de informática no Brasil, p. 87, referem as duas posições, a "dos que consideram o crime de informática como outro crime qualquer, perfeitamente tipificável em face da atual legislação criminal", não havendo "necessidade, por exemplo, de discutir-se entre a tutela garantidora da informação contida em um documento qualquer e a informação contida em um computador." Este representaria "apenas um instrumento facilitador na prática de um crime já previsto anteriormente pela lei penal". O "segundo grupo", dizem eles, "abrange os que consideram que as medidas legais existentes são insuficientes para lidar com esse tipo de ameaça, e proclamam a necessidade de urgente adaptação da legislação existente com a introdução de uma legislação para combater o problema". Ver, ainda, sobre as duas orientações Gustavo Arocena, Los delitos informáticos, p. 44-6.

34 Neste sentido o Projeto de Lei 1521/91, do então senador Maurício Correia, que considera crime contra a inviolabilidade de dados e sua comunicação o ato de violar dados por meio de acesso clandestino ou oculto a programa ou sistema de comunicação.

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 para fins determinados"[35]. Trata-se da Lei n ° 9609, de 9 de dezembro de 1998, que contempla normas de proteção a programas de computador, e, no artigo 12, define crime contra o direito do autor. Fernando Galvão da Rocha, examinando a lei anterior (Lei 7646, de 18/12/98), lembra que atinge crimes como o decorrente da cópia dos programas de computador, atividade conhecida como "pirataria", a qual, "apesar de ilícita, vem se constituindo um hábito cada vez mais comum em nossa sociedade. Desde usuários domésticos até grandes empresários, a cópia de programas é tão difundida quanto a cópia xerox de textos publicados em livros ou periódicos". Para objetivar maior proteção aos programas, a Lei 7646/87, diversamente da proteção do direito autoral, incrimina a "conduta de quem copia programa de computador, mesmo que para uso próprio e sem fins lucrativos"[36]. A nova lei pune, de maneira genérica, a "violação dos direitos de autor de programa de computador", e, de forma mais grave, a violação consistente em "reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente", ou, ainda, a atitude de quem "vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral" (art. 12 e § § 1 ° e 2 °).

Também se encontra referência à programa de computador no artigo 2°, inciso V, da Lei 8137, de 25 de dezembro de 1990, dos crimes contra a organização da ordem tributária e econômica, que pune a seguinte conduta: "Utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública". A proteção, aí, é dirigida à Fazenda Pública, não ao contribuinte.

A violação de sigilo de operação ou de serviço prestado por instituição financeira ou integrante do sistema de distribuição de títulos mobiliários constitui o crime previsto no art. 18, a Lei 7.492, de 16.6.86.

No tocante aos crimes contra a segurança nacional, a ordem política e social, o artigo 13, da Lei 7.170, de 14.12.83, pune a conduta de comunicar, entregar, permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados que, no interesse do Estado brasileiro, como sigilosos. Também se pune quem "obtém ou revela, para fins de espionagem, informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, e instalações ou de sistemas de processamento automatizados de

---

[35] Essa definição é da própria Lei 9609, contida nas Disposições Preliminares, artigo 1 °.

[36] Fernando Galvão da Rocha, Criminalidade do computador, p. 525.

dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devam permanecer em segredo"[37].

Mas, como inexiste lei específica de proteção a dados[38] ou informações[39] computadorizados, necessário se recorrer ao Código Penal e a outros textos legislativos, na tentativa de enquadrar as condutas ilícitas cometidas, abranjam crimes informáticos "puros" ou "impuros".

Lembra Maria Helena Junqueira Reis casos de **subtração do disco rígido ou das informações registradas**. Haveria crime de furto? Quanto ao disco rígido, sem dúvida. O problema está em verificar se o "dado" constante do computador é "coisa móvel". A autora cita Casabona, para quem não é possível o enquadramento da conduta de subtração de informes registrados no computador, pois estaria sendo utilizada analogia "in malam partem", vedada no Direito Penal. Refere, ainda, possível adequação no artigo 155, § 3 °, do Código Penal, porque as informações dentro do computador tornam-se "impulsos elétricos". Ela contesta, contudo, afirmando que a "energia elétrica usada em um computador é coisa ínfima. A informação que está num meio magnético nada tem a ver com a produção de energia elétrica ou outra qualquer. Ela tem um valor próprio, torna-se impulso elétrico para fins de processamento. " Na mesma linha, Fernando Galvão da Rocha, entende que as "informações constantes em um sistema de computador não poderão ser alvo de subtrações, salvo quando também o seja seu suporte físico", isto porque, as "informações são bens imateriais de impossível apreensão"[40].

Outro questionamento surge quanto ao enquadramento da **fraude por manipulação de dados do computador**. Divergem os autores. Para Casabona,

---

[37] Ver Fernando Galvão da Rocha, Criminalidade do computador, p. 528-9.

[38] Dados são, segundo Fernando Galvão da Rocha (Criminalidade do computador, p. 527), "elementos básicos de informação, caracteres ou símbolos que são fornecidos ou produzidos por um computador. Representam fatos, conceitos ou instruções de maneira convencional e apropriada para comunicação, interpretação ou processamento por meios automáticos". Servem "para indicar o registro de fatos e valores produzidos por um acontecimento, uma atividade ou uma situação". Isoladamente, "possui significado restrito", mas, "associado a outros se converte em informação útil". Ainda, o "banco de dados é um conjunto específico que reúne uma coleção de dados ou informações já obtidas".

[39] A informação é, para Fernando Galvão da Rocha (Criminalidade do computador, p. 527), "o resultado do processamento de vários dados, que envolve técnicas de seleção, relacionamento, interpretação e cálculo de dados elementares". Otto Banho Licks e João Marcelo de Araújo Júnior (Aspectos penais dos crimes de informática no Brasil, p. 91-2) referem o dado e a informação. Definem o dado "como qualquer parte de uma informação, ou como algo que tem o poder de trazer qualquer informação. Também pode significar, quando relacionado com computadores e informática, uma informação numérica de formato capaz de ser entendido, processado ou armazenado por um computador ou parte integrante de um sistema de computador. Ou ainda, uma informação preparada para ser processada, operada ou transmitida por um sistema de computador ou por um programa de computador. Os dados podem expressar fatos, coisas certas ou comandos e instruções. "Informação", por sua vez, é algo através do qual se adquire alguma forma de conhecimento. É comumente referida como uma coleção de dados que descreve ou integra um corpo de conhecimentos". Os dados servem, dizem ainda, como suportes dos objetos imateriais, subjetivos que são as informações."

[40] Fernando Galvão da Rocha, Criminalidade do computador, p. 529.

nestas manipulações não há pessoa induzida a erro, principalmente quando se realizam na fase da programação ou processamento dos dados, só sendo detectadas quando o prejuízo já tenha se consumado. Na mesma linha, João Marcelo de Araújo Júnior no relatório apresentado porque faltaria a encenação característica da fraude comum. Em contrário, Ivete Senise Ferreira[41] e Valdir Sznick[42]. Assim também nos parece. O fato de existir dados alterados faz com que a pessoa opere o computador sem conhecimento da manipulação realizada, e, assim, está agindo por erro, ao qual foi levada mediante artifício

Nos casos de **sabotagem ou inutilização de dados ou programas**, o crime seria de dano. Esclarece Fernando Galvão da Rocha que a informação, em si, não é documento, nem coisa, e, assim, não pode ser objeto de crime de dano, supressão ou falsidade documental. Contudo, diz ele, "considerando que o equipamento do computador é coisa alheia móvel e que as condutas de apagar ou alterar suas representações digitais repercutem diretamente nas condições de seu funcionamento, é possível a caracterização de dano. O objeto da tutela não é as representações digitais das informações, mas o seu equipamento de computador, que será deteriorado em seu desempenho"[43]. Também configurariam dano os males causados ao computador pela utilização de "vírus", "uma vez que o equipamento seria deteriorado pela inviabilidade de seu normal funcionamento"[44] [45].

Nos **serviços bancários** foi crescente a utilização de cartões magnéticos e de senhas como mecanismos protetores aos clientes que realizam operações de depósito, pagamento e saque através de sistemas de computadores. Contudo, tais mecanismos não impediram que fosse rompida a segurança por eles pretendida, através de ingresso indevido no sistema. Para Fernando Galvão da Rocha, "o agente que supera os mecanismos de proteção dos sistemas bancários, através da utilização dos cartões de identificação ou senhas, para transferir valores para conta-corrente na qual poderá efetuar saque, ou autorizar diretamente este saque, pratica estelionato previsto no art. 171 do CP, uma vez que com a conduta o agente obtém vantagem ilícita em prejuízo alheio, mediante a utilização de fraude que vicia o consentimento do operador financeiro para a entrega dos valores. Nessa hipótese, não há subtração do dinheiro que porventura exista em conta bancária, mas a enganosa entrega pela instituição financeira, que acredita realizar operação autorizada pelo titular da conta[46]. Também Damásio entende que a "entrada no

---

[41] Ivete Senise Ferreira, Os crimes da informática, Revista de Estudos Jurídicos em homenagem a Manoel Pedro Pimentel, p. 139 e seguintes

[42] Valdir Sznick, O delito e o computador, Revista Trimestral de Jurisprudência dos Estados, ano 8, v. 26, jan./mar. 1984.

[43] Fernando Galvão da Rocha, Criminalidade do computador, p. 529.

[44] Fernando Galvão da Rocha, Criminalidade do computador, p. 531.

[45] Sobre o crime de dano na informática escreveu Carlos María Romeo Casabona o artigo "Los delitos de daños en el ambito informativo", Derecho Penal y Criminologia, Revista del Instituto de Ciências Penales y Criminologia, Bogotá, v. 13, n. 43, p. 45-70, jan./abr. 1991.

[46] Fernando Galvão da Rocha, Criminalidade do computador, p. 530.

sistema de informações de um banco com a efetiva transferência de valores pode ser punida como estelionato"[47].

Em matéria da Folha de São Paulo (Crime.com.br), foram relacionados quatro tipos de **golpes** utilizados em crimes através de computador e relacionados com os **serviços bancários**: 1. Grampo de teclado; 2. Golpe do cadastro; 3. Invasão do computador; 4. Grampo de telefone. O grampo de teclado permite que, no momento da digitação, sejam captados alguns dados que ficam retidos na memória, número da conta e senha inclusive. No golpe do cadastro, a pessoa consegue desviar dinheiro da conta do correntista ainda que ele não utilize o sistema para movimentação financeira; com a senha, a pessoa realiza o cadastro e, com isso, realiza operações bancárias, até mesmo transferências. A invasão do computador é o ingresso no computador, tendo acesso a programas. Por fim, utiliza-se o sistema de telefonia para obtenção da senha, através do grampo de telefone, o que se realiza através de um computador ou pelos tons.

Fala-se que atualmente, "um dos **golpes** mais aplicados no **sistema bancário** é o chamado "salami slicing" (fatias de salame)", em que, por recursos diversos, os agentes "realizam transferências eletrônicas de pequenas quantias, de milhares de contas"[48]. Os jornais vêm noticiando, além desta forma, outros golpes, com transferências de dinheiro para determinadas contas[49]. Os bancos estão reforçando seus sistemas para diminuir as chances de ataques e movimentação indevida de contas[50].

Têm sido considerados **crimes de violação de correspondência** os casos "de **invasão de caixa postal**" e **crimes contra a honra** as "**ofensas por meio do e-mail**"[51]. Houve, recentemente, caso em que a ex-esposa através de "e mail" enviou a terceiros mensagens eletrônicas com dizeres difamatórios ao ex-marido; a questão foi levada ao Tribunal de Justiça do Distrito Federal que determinou que ela não mais enviasse a mensagem; a matéria foi encaminhada ao Supremo Tribunal Federal, ainda não sendo julgada. Discutem-se, aí, dois direitos: o direito que todos têm à proteção de sua honra e o direito a que todos têm de não ver a sua caixa postal devassada, assim como não se permite a inviolabilidade da correspondência[52].

Também pode estar ligado a crimes por computação a **concorrência desleal** que se estabelece entre empresas produtoras de *software*, definido no Código de Propriedade Industrial[53].

---

47 Damásio, Gazeta Mercantil, 5 de maio de 1999.

48 Estado de São Paulo, 14 de junho de 1999, C2.

49 Ver reportagens, intituladas Crime.com.br, feitas pela Folha de São Paulo no dia 22.11.98,

50 A Gazeta Mercantil de 5 de maio de 1999 informou das medidas usadas pelo Banco do Brasil e dos maiores bancos do países para reforçar a segurança nos seus sistemas.

51 O Estado de São Paulo, 14.6.99, C2.

52 Folha de São Paulo, 22.3.99, 1-2.

53 Fala a respeito deste crime Fernando Galvão da Rocha, Criminalidade do computador, p. 526.

Bastante noticiado foi a utilização de computadores para divulgação de imagens obscenas, com cenas envolvendo crianças (**pedofilia**). Fala-se na possível definição como crime de ato obsceno pelo Código Penal e, quando veicula imagem de criança, em ofensa ao Estatuto da Criança e do Adolescente[54].

São divulgados crimes que interferem diretamente na **entrada, saída ou armazenamento de dados ou no uso da Internet**, como o grampo de teclado, em que se utiliza a memória; o golpe do cadastro, atingindo pessoa que nunca usou o sistema informatizado de banco; o grampo de telefone[55].

4. Aspectos processuais

Os crimes praticados por computador podem ser de ação penal pública ou privada.

São de ação penal privada os crimes relativos à violação de direito autoral de programa de computação e o de concorrência desleal entre empresas produtoras de *software*. O mesmo sucede com eventual enquadramento dos crimes como delito de dano definido no Código Penal. Nestes casos, importante é identificar o sujeito passivo, pois a ele incumbirá promover a ação penal[56].

O maior problema está na apuração dos crimes, o que é sempre ressaltado por todos os que estudam os crimes praticados por computador[57].

O criminoso que atua pelo computador não aparece, usa a tecnologia a seu favor. Manoel Camassa bem acentua que esse criminoso, por ele denominado de

---

[54] A questão já foi levada ao Supremo Tribunal Federal, através do "habeas corpus" n ° 76.789-PB. Entendeu-se que o crime de veiculação de cenas de sexo infanto-juvenil devido sua inserção na rede Internet configura o crime do artigo 241 do E.C.A. Disse o Ministro Relator que o "tipo cogitado - na modalidade de "publicar cenas de sexo explícito ou pornográfica envolvendo criança ou adolescente"- ao contrário do sucede por exemplo aos da Lei de Imprensa, no tocante ao processo de publicação incriminada é uma norma aberta: basta-lhe a realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BNS/Internet de Computador. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreende na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de intervenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito a que nele se compreendia a morte dada a outrem mediante arma de fogo" (Informativo STF n ° 130, 11.11.98). Contudo, para Maurício Ribeiro Lopes, o Estatuto da Criança e do Adolescente não se refere a uso de rede de computador e, assim, não há precisa definição do crime (Folha de São Paulo, 10.10.98, 3-2).

[55] Folha de São Paulo, 22.11.98, 3-2.

[56] Ver sobre identificação do sujeito passivo nos crimes de violação de direitos de programas Fernando Galvão da Rocha, Criminalidade do computador, p. 526-7.

[57] Fala Pérez Luño, Manual de Informática y derecho, p. 76, que a "criminalidade informática se caracteriza pelas dificuldades de descobri-la, prová-la e persegui-la. Referem, em entrevista para a Gazeta Mercantil, em 5 de maio de 1999, essa dificuldade na apuração dos crimes informáticos Otto Steiner, advogado com larga experiência com instituições financeiras, o advogado criminalista Antonio Sérgio Pitombo e o juiz aposentado e consultor jurídico Luiz Flávio Gomes.

criminoso invisível ou criminoso virtual, está escudado no anonimato[58]. Por isso, dificilmente haverá reconhecimento do agente. Nos casos em que a pessoa ingressa no computador alheio pela Internet ou via "modem" e manipula informações, a sua identificação é muito difícil.

Com base em pesquisa realizada pela polícia dos Estados Unidos fala-se que o "autor do crime digital é jovem, inteligente, com idade entre 16 e 32 anos" e que "é movido pelo desafio da superação do conhecimento e além do sentimento do anonimato". Já se tem atribuído a ele a denominação de "cybercriminoso"[59].

A incorporação dos dados computadorizados ao processo, segundo Miguel Angel Torrès Morato, pode se concretizar por duas formas: a) a apreensão física do objeto no qual consta a informação; a intervenção no processo de comunicação com o fim de captar o conteúdo do dado. Salienta, contudo, que o juiz deve ser muito cauteloso, ao autorizar a apreensão ou a interceptação, sopesando em face do critério da proporcionalidade os interesses em jogo, tendo em conta que o conhecimento da grande quantidade da dados contidos no material apreendido ou interceptado pode causar dano irreparável à pessoa investigada[60].

Entre nós, há que se examinar a possibilidade da apreensão dos dados do computador à luz da Constituição Federal.

Segundo o artigo 5 °, inciso XII, da Constituição, os dados são invioláveis. Tal dispositivo, após arrolar várias inviolabilidades, só abriu exceção para as interceptações telefônicas, permitindo que, mediante autorização judicial e para fins criminais, pudesse ser realizada. Há, contudo, orientação no sentido de que essa autorização atingiria também os dados em virtude da redação dada ao dispositivo[61]. Saliente-se, por outro lado, que a restrição é dirigida à proteção do indivíduo, não albergando assim os dados de computadores de empresas ou de órgãos públicos.

A Lei de Interceptações Telefônicas (Lei 9296/96), em seu artigo 1°, permitiu a interceptação em caso de telemática. Aí podem ser enquadradas condutas consistentes na transmissão de dados por computador. A possibilidade de, com autorização judicial, ser feita a interceptação da comunicação de dados de computador facilita a apuração dos crimes. Há contudo entendimento no sentido de ser esse dispositivo inconstitucional porque teria ido além do texto constitucional, o qual só autorizaria a interceptação das comunicações telefônicas feitas sem a interferência do computador. Vem, contudo, firmando-se outro entendimento: se é permitida a interceptação telefônica entre duas pessoas diretamente porque não se

---

[58] Manoel Camassa, A tecnologia mudando o perfil da criminalidade, Revista Brasileira de Ciências Criminais, ano 7, n. 25, jan-mar 1999, p. 226-239.

[59] O Estado de São Paulo, 14.6.99, C2.

[60] Miguel Angel Torres Morato, La Prueba Ilícita Penal, p. 280.

[61] A questão foi por nós estudada no livro 'Processo Penal Constitucional", a ser editado pela Revista dos Tribunais.

permitir a interceptação quando, mediante uso telefone, há comunicação entre dois computadores[62].

Superados esses óbices constitucionais, outras dificuldades podem prejudicar a apreensão dos dados computadorizados. Estes podem ser facilmente apagados e, assim, se houver qualquer desconfiança do agente de que está sendo objeto de investigação, ele certamente impedirá, com o apagamento dos registros, qualquer investigação. Daí a necessidade do maior sigilo.

Os registros computadorizados constituirão prova documental. Se impressos, o material resultante da impressão também será documento. Este deve ser periciado juntamente com os dados resultantes da apreensão para prova da materialidade, ficando assentada a relação existente entre o documento impresso e os dados apreendidos. Quando se tratar de códigos de comunicação diversos do alfabeto, haverá necessidade de a perícia esclarecer seu significado após a impressão[63].

A prova testemunhal nesses crimes só será útil quando, de alguma forma, o agente tenha comentado com alguém a respeito de sua conduta ou tenha sido visto na prática delituosa. Trata-se, contudo, de ocorrência difícil. Quem age criminosamente, normalmente não alardeia sua conduta, principalmente o criminoso do computador, pessoa dotada de conhecimento superior ao da média dos delinqüentes.

Nos crimes praticados pela Internet, a atuação persecutória depende muito da colaboração de provedores e que, muitas vezes, não se encontram no país onde a ação delituosa apresenta resultados. Negam, em regra, informações com o argumento de que dependem de uma autorização judicial em virtude do sigilo. Por isso, há tentativa, como nos Estados Unidos, de alteração na legislação a fim de que os "provedores de acesso possam liberar informações sobre usuários, para que os "hackers" sejam rastreados"[64].

Questão relevantíssima é a da competência.

Os crimes por computador são crimes em que o agente está em um local e o resultado é produzido em outro, no mesmo país ou em país diverso.

A competência, dentro do país brasileiro, será determinada pelo local da consumação, aquele em que se produz o resultado. Quando se trata de delito que

---

[62] Também essa questão da constitucionalidade do artigo 1 °, da Lei de Interceptações Telefônicas, foi por nós analisada no livro "Processo Penal Constitucional".

[63] Os registros, vistos como prova, são considerados documentos, mas, na falta de previsão expressa, não se pode falar em falsidade documental quando sejam alterados os dados nele contidos. Estendeu, contudo, o conceito de documento sentença proferida na Espanha e citada por Miguel Angel Torres Morato, La Prueba Ilícita Penal, p. 275, condenando por delito continuado de falsidade documental funcionário de banco que manipulou as contas correntes de diversos clientes. Posteriormente, lembra o autor, o Código Penal de 1995, de forma expressa, incluiu na definição de documento todo suporte material que expresse ou incorpore dados, fatos ou narrações com eficácia probatória.

[64] Folha de São Paulo, 19 de junho de 1999, 1-7.

envolva dois ou mais países a competência se soluciona pelas regras de direito internacional. Para Valdir Sznick seriam competentes os foros dos locais da idealização e da execução do crime, como o local em que veio o crime a produzir seu resultado[65].

A necessidade de expedição de rogatória tem, também, contribuído para dificultar a investigação e apuração dos crimes informáticos. Como muitas vezes o crime é praticado por pessoa que se utiliza de provedor estrangeiro ou se encontra em outro país surge a necessidade de providências nesse país, com necessidade de expedição de rogatória, principalmente se há necessidade de cumprir ordem de juiz brasileiro. Nesse ponto, seria possível pensar em convênios ou, até mesmo, na criação de sistema de cooperação internacional em que os cumprimentos de ordens judiciais em outros países pudessem ser feitos de maneira mais rápida. Noticia-se que alguns provedores têm aceitado as ordens expedidas por juízes brasileiros[66].

Essa internacionalização do crime de informática e que reflete na investigação, no processo e na determinação da competência, insere-o no que se vem denominando Direito Penal da Globalização, ou seja, "direito marcado pela uniformização, pela criação de novos tipos penais, em especial no campo sócio-econômico"[67]. Essa uniformização, além de ser legislativa, deve abranger também a formação de operadores de direito preparados para a criminalidade global: policiais, promotores, juízes. Ainda, pela rapidez do desenvolvimento tecnológico, faz-se mister o intercâmbio de conhecimentos. Também há necessidade de eficientes sistemas de cooperação entre os países, principalmente na investigação dos crimes. Por tudo isso, na Europa, há forte movimento na busca de maior identidade na legislação e na atuação conjunta para os crimes internacionais, entre ele o crime informático. Fala-se mesmo em um tribunal comunitário.

Mas, enquanto avança a criminalidade por computador, tornando-se cada vez mais sofisticada e utilizando-se de pessoas experientes, diz Manoel Camassa que a polícia não consegue acompanhar esse caminhar. Os recursos técnicos são "quase os mesmos de mais de meio século atrás", há "falta ou deficiência de material", impõe-se melhor "qualificação profissional para atuar nas diligências e elaboração dos laudos periciais, com a mesma capacidade e competitividade que a própria inteligência dos agentes ou dos instrumentos utilizados para a prática dos crimes modernos, os aqui denominados delitos virtuais"[68].

Apesar de todas as dificuldades, algumas medidas têm sido tomadas pelos órgãos encarregados da persecução penal e tem sido noticiada atuação eficaz da polícia no desvendamento de alguns crimes praticados por computador, sempre, contudo, com a alusão às grandes dificuldades encontradas.

---

[65] Valdir Sznick, O delito e o computador, p. 51.

[66] O Estado de São Paulo, 14.6.99, C2.

[67] Jésus-Maria Silva Sánchez, In Folha de São Paulo, 12.9.98, Cad. 3, p. 2.

[68] Manoel Camassa, A tecnologia mudando o perfil da criminalidade, p. 228-9.

A Polícia Federal criou uma divisão para investigar crimes por computador, ligada ao Instituto Nacional de Crimalística (INC) com o nome de Divisão de Crime por Computador. Aí atuam três peritos que fizeram cursos específicos nos Estados Unidos. Tem ainda se dedicado especialmente aos casos de utilização da Internet para pedofilia, para difusão de orientações sobre a fabricação de bombas e outros tipos de explosivos caseiros, principalmente quando envolvam criminalidade internacional. Alguns crimes foram deslindados, como o encontro de bombas caseiras em escolas de Brasília onde estavam sendo realizadas provas do vestibular da Universidade de Brasília[69] [70].

Em São Paulo, a Polícia Civil criou uma página na Internet e dispõe de um e-mail, no qual tem recebido muitas denúncias anônimas, as quais têm ajudado no desvendamento de alguns crimes. Também a Associação Brasileira de Provedores de Internet mantém, em parceria com o Ministério Público de São Paulo campanha sobre a pornografia infantil em computador, estimulando denúncias pela rede.[71] Na polícia paulista, o delegado Mauro Marcelo de Lima e Silva estaria se dedicando à apuração desses crimes.

Em virtude de investigação realizada pela Polícia Civil de São Paulo sobre uso indevido de 40 sites, que divulgavam pedofilia, orientações sobre como fazer bombas e praticar atentados, os sites foram fechados. Só houve identificação dos autores em dez casos. Na maioria a divulgação era feita em "home pages" hospedadas em provedores estrangeiros, americanos e europeus. Alguns aceitaram decisões de juízes brasileiros. Além desses, outros 'sites" já haviam sido fechados[72].

A Polícia Civil do Mato Grosso do sul prendeu em flagrante pessoas que utilizavam a Internet para a veiculação de shows eróticos ao vivo. Houve apreensão do equipamento de informática montado para transmitir os shows. O fato foi enquadrado no artigo 234 do Código Penal que considera como criminosos os atos de "fazer, importar, exportar, adquirir ou ter sob sua guarda para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto erótico"[73].

Para descoberta das pessoas que transmitiam cenas de sexo com crianças pelo computador houve operação conjunta de vários países e que culminou na prisão de cerca de cem pessoas no ano de 1998. Atuaram policiais dos Estados Unidos, da Inglaterra, Escócia, Alemanha, Itália, Noruega, Bélgica, Finlância,

---

[69] Folha de São Paulo, 26.3.99, A9 e Estado de São Paulo, 14.6.99, C2.

[70] O Estado de São Paulo, 14.6.99, C2, menciona com base em informação do Delegado paulista Mauro Marcelo de Lima e Silva que "nos Estados Unidos, Inglaterra, Canadá, o FBI, a Scotland Yard e a Real Polícia Montada está formando ... policiais especialmente treinados para combater os crimes digitais".

[71] Folha de São Paulo, 4.8.98, 3-8, e 10.10.98, 3-2.

[72] Folha de São Paulo, 4.8.98, 3-8.

[73] Folha de São Paulo, 3.6.99, 3-2.

Áustria, França, Suécia e Portugal. Houve apreensão de grande quantidade de revistas, fitas de vídeo e CD-Roms[74]. Falando a respeito, diz Manoel Camassa que "a polícia britânica, auxiliada pela Polícia de outros 21 países, em uma gigantesca operação internacional sem precedentes, conseguiu desbaratar uma gangue de pedófilos que divulgavam fotos pornográficas com menores via "Internet". Salienta, então, que as "pessoas envolvidas neste tipo de atividade obscena se sentiam até agora relativamente impunes, certas de que esse canal da informática não sofre controles, o que, como se vê, tanto aqui como lá, há a tipificação penal e, portanto, a necessidade de repressão"[75].

Noticiou-se, entre nós, condenação pelo Tribunal de Alçada Criminal em caso de crime praticado por computador. O agente entrou no computador de um banco, transformou ações ao portador que não eram reclamadas em nominativas e remeteu o dinheiro para sua conta. Fora condenado em primeira instância por furto. O tribunal manteve a condenação, mas alterou a classificação para estelionato[76]

Enfim, há um novo caminho a ser percorrido.

O primeiro passo é a busca de especialização principalmente no tocante à investigação dos crimes por computador.

Ainda, para evitar dificuldades no enquadramento há necessidade de legislação específica. Entre outros, poderia ser definido tipo semelhante ao de furto, consistente na subtração de informações registradas. Importa tornar crime a simples conduta de acesso a computador quando não tenha havido autorização ou não esteja aberto à comunicação, quando, por exemplo, está resguardado por "senha". Seria de todo interesse definir melhor o documento para fins penais e processuais penais, aí incluindo os registros magnéticos, regulando-se a forma de apreensão e de realização de perícia.

---

[74] Folha de São Paulo, 10.10.98.

[75] Manoel Camassa, A tecnologia mudando o perfil da criminalidade, p. 234-5.

[76] Folha de São Paulo, 22.11.98, 3-3.