Os objetos intangíveis na era da criminalidade informática

Roberto Chacon de Albuquerque[*]

Resumo

Neste artigo analisa-se a proteção dos objetos intangíveis em sede de criminalidade informática, com base no direito alemão e no direito holandês. Este trabalho delimita o conceito de crime informático, distinguindo suas principais características. Diferenciando objetos tangíveis de objetos intangíveis, o artigo defende a reforma da legislação penal com fundamento em interesses jurídicos merecedores de proteção específica.
Palavras-chave: Objetos tangíveis. Crime. Criminalidade. Informática.

* Advogado, Doutor em Direito pela FDUSP, professor universitário da Universidade Católica de Brasília; r_albuquerque@hotmail.com

1 INTRODUÇÃO

Todos os Códigos Penais, nos mais variados países, têm protegido, ao longo da história, sobretudo, os objetos tangíveis. A proteção dos dados armazenados, processados ou transmitidos por sistemas informáticos, bem como de outros objetos intangíveis, tornou-se prioritária a partir da segunda metade do século XX. Com a emergência da sociedade pós-industrial, capitaneada até agora pela indústria da informática, tais dados têm assumido um valor cada vez maior. A mudança de paradigma, da proteção dos objetos tangíveis para a dos objetos intangíveis, levou a que vários países tenham submetido sua legislação penal a alterações. A vedação à analogia *in malam partem* pode oferecer empecilhos para que se submetam a tipos penais tradicionais, como o estelionato, até mesmo novas condutas ilícitas em que a informática é utilizada como meio *sui generis* para praticar-se o crime.

Houve, até agora, três grandes levas de reforma da legislação penal. A primeira correu no campo da proteção à privacidade, no decorrer já da década de setenta, tendo sido uma reação aos riscos apresentados pela tecnologia da informação à proteção à intimidade. Alemanha, Austrália, Áustria, Canadá, Dinamarca, Estados Unidos, Finlândia, França, Irlanda, Israel, Japão, Luxemburgo, Noruega, Nova Zelândia, Países Baixos, Reino Unido e Suécia, todos adotaram leis específicas para proteger o cidadão do armazenamento, coleta e transmissão arbitrários de dados pessoais. (SIEBER, 1990, p. 120). A segunda leva compreendeu a reforma legislativa envolvendo a tipificação de crimes informáticos com natureza econômica, com projeção patrimonial, tendo início em princípios da década de oitenta. Ao invés de estender o significado das disposições legais já existentes, o que contradiria os princípios da legalidade e a proibição da analogia *in malam partem* em sede de direito penal, muitos países preferiram promulgar leis específicas sobre criminalidade informática, tipificando, inclusive, o acesso não-autorizado a sistemas informáticos. Esse esforço foi considerado necessário, porque tais espécies de crimes envolviam novos métodos para a prática de crimes tradicionais − induzir em erro um computador, não uma pessoa − (SIEBER, 1990, p. 121), bem como objetos intangíveis – dados armazenados, processados ou transmitidos por sistemas informáticos −. Alemanha, Austrália, Áustria, Canadá, Chile, Dinamarca, Estados Unidos, França, Grécia, Itália, Japão, Noruega, Suécia e Reino Unido seguiram esse caminho (SIEBER, 1990, p. 121). Ao longo da década de oitenta, uma terceira leva de reformas incrementou a proteção à propriedade intelectual. Depois da exclusão dos programas de computador da proteção conferida pelo direito das patentes, ocorrida nos anos 70, o software passou a ser considerado uma obra intelectual, à luz do direito autoral, na Alemanha, Austrália, Canadá, Chile, Dinamarca, Estados Unidos, Filipinas, França, Hungria, Índia, Israel, Japão, México, Reino Unido e Suécia. (SIEBER, 1990, p. 122). Desde 1984, a Alemanha, Dinamarca, Estados Unidos, França, Itália, Japão, Países Baixos, Reino Unido e Suécia aprovaram legislação específica para a proteção de produtos semicondutores. (SIEBER, 1990, p. 122).

O Brasil, até agora, atendeu, apenas parcialmente, ao disposto na primeira, na segunda e na terceira levas de reformas. A Constituição Federal, promulgada em 5 de outubro de 1988, determinou em seu art. 5º, LXXII, que o *habeas data*, regulamentado posteriormente pela Lei 9.507/97[1] (BRASIL, 1997), constitui um instrumento de defesa dos direitos individuais e coletivos[2] (BRASIL, 1988). A Lei 9.983/00[3] (BRASIL, 2000) com relação à qual já manifestamos nossas reservas, que serão aprofundadas mais adiante, introduziu no Código Penal uma série de dispositivos que enquadram os funcionários públicos que tenham, por exemplo, inserido ou alterado dados armazenados, processados ou transmitidos por sistemas informáticos[4]. A Lei 9.609/98[5] (BRASIL, 1998), artigo 2º, *caput*, prevê que "o regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei".

São, basicamente, dois os métodos de reforma legislativa. O primeiro é baseado numa reforma do Código Penal. Novos artigos são introduzidos nele, que passa a oferecer proteção contra condutas ilícitas denominadas, como tivemos a oportunidade de conferir an-

teriormente, de estelionato informático, violação de segredo informático etc. Esse foi o caminho seguido, por exemplo, pela Alemanha, Áustria, Bélgica, Dinamarca, França, Grécia, Noruega, Países Baixos, Suécia e Suíça. O segundo método consiste na adoção de uma legislação específica, desprendida do todo orgânico do Código Penal. Portugal[6] e Reino Unido[7] adotaram esse método, a par de vários outros países (BOXTEL, 1990, p.20). A Austrália e os Estados Unidos dispõem de uma legislação sobre criminalidade informática tanto estadual como federal (BOXTEL, 1990, p. 20). Acreditamos que a primeira opção, por sua organicidade, seja a mais adequada para o Brasil − definir que condutas devem ser consideradas crimes − para sua posterior inserção no Código Penal. Devemos verificar em que medida podemos conferir uma nova roupagem a artigos já existentes no Código, se eles devem ser atualizados para enquadrar condutas que envolvam novos métodos, com auxílio da tecnologia da informação, para a prática de crimes tradicionais, bem como para oferecer proteção a objetos intangíveis. Os tipos penais a serem criados devem seguir a sistemática consagrada em tipos já existentes, mas com outros elementos constitutivos, sob a forma de artigos independentes.

A colaboração penal internacional é fundamental para que protejamos a sociedade da criminalidade informática. Convém aprovar tipos penais que sejam compatíveis com os já consagrados na comunidade internacional. Em decorrência da interconectividade, com pessoas situadas em diferentes países compartilhando dados simultaneamente, em tempo real, os crimes informáticos possuem uma projeção internacional ímpar. São crimes transnacionais por excelência, cuja prática pode ter efeitos diretos ou indiretos envolvendo mais de um país. Os ataques de *hackers* revelam a possibilidade de cometer-se uma infração num determinado país, enquanto os efeitos decorrentes dessa infração podem repercutir diretamente noutros países. A par da adoção de artigos específicos sobre crimes informáticos, devemos fomentar a celebração de acordos bi- e plurilaterais, privilegiando a adoção de medidas de cooperação, prevenção, repressão e treinamento, entre os respectivos países-membros.

2 CONCEITO DE CRIME INFORMÁTICO

A informática[8] constitui uma parte integral da vida quotidiana. Os sistemas informáticos tornaram-se um instrumento indispensável de trabalho. Sua influência sobre o conteúdo, espaço, forma e tempo das atividades desempenhadas habitualmente, sobre o desenvolvimento da ciência e da indústria, sobre o funcionamento das empresas e repartições públicas, e sobre sistemas de telecomunicação tem transformado a vida moderna. A tecnologia da informação trouxe uma grande quantidade de benefícios tanto para o setor público como para o privado, bem como para o próprio cidadão. Seu impacto positivo não deve ser medido apenas em termos de tempo e dinheiro. Os sistemas informáticos podem ter, também, uma projeção libertária, ao assumir tarefas repetitivas e ausentes de criatividade, que podem tornar qualquer atividade desinteressante. Ao mesmo tempo, uma evolução tão rápida e fundamental desperta temores de natureza socioeconômica[9] ou jurídica[10]. A informática oferece oportunidades altamente sofisticadas para a prática do crime. Computadores podem ser utilizados para simplificar a prática de crimes clássicos, como os crimes contra a honra.

O direito penal não está aparelhado adequadamente para fazer frente à criminalidade informática. Isso cria uma incerteza na sociedade sobre o que é e o que não é permitido. Ele pode delimitar com clareza o que pode e o que não pode ser feito com a tecnologia da informação, contribuindo para criar entre os usuários da informática uma consciência sobre as regras jurídicas que devem ser respeitadas[11]. Para evitar decepções com a aplicação do direito penal, para que ele não se transforme num tigre de papel, deve-mos adotar uma posição realista. Precisamos nos concentrar nos interesses jurídicos vitais a serem protegidos. Mesmo assim, não devemos esperar milagres. Embora ele possa desestimular a criminalidade informática, o direito penal não pode evitar que seus preceitos sejam infringidos. Um aspecto fundamental é como a sociedade encara a criminalidade informática. Ela pode tolerar essa criminalidade, ou mesmo a estimular, a despeito do previsto pelo direito penal. A repressão à criminalidade informá-

tica tampouco se esgota no processo de tipificação das condutas correlatas. Ela pode terminar sendo desprovida de qualquer sentido, caso não sejam levadas em conta questões como cooperação internacional e aperfeiçoamento técnico dos aparatos judicial e policial.

Qualquer tentativa de definir o termo "crime informático", de conceituá-lo, apresenta desvantagens. Dificilmente, pode ser elaborada uma definição sucinta e precisa sem que deixemos dúvidas quer com relação ao seu objeto, quer com respeito à própria utilização da definição que lhe for conferida. A noção de crime informático envolve várias espécies de crimes. Não devemos adotar uma definição formal, estática, o que pode criar mais confusão do que soluções. Tem havido a tentativa de definir "crime informático" de várias maneiras. Por exemplo, como qualquer conduta ilícita na qual um sistema informático constituir um instrumento ou objeto de um crime. Noutras palavras, qualquer crime cujo meio ou objetivo for influenciado por um computador, qualquer atividade ilícita associada a um sistema informático na qual o sujeito passivo perca ou possa ter perdido algo, e o sujeito ativo tenha, deliberadamente, ganha ou possa ter ganho algo[12]. A Organização para Cooperação e Desenvolvimento Econômico (OCDE) adotou a seguinte definição: "Considera-se abuso informático qualquer comportamento ilícito, aético ou não autorizado relacionado ao processamento automático e à transmissão de dados."[13] Essa definição tampouco resolve a questão, apresentando vários problemas. A primeira parte da definição − "qualquer comportamento ilícito, aético ou não autorizado" −, extremamente ampla, inclui condutas que não podem ser consideradas crimes, por mais repreensíveis que sejam. A segunda parte – "relacionado ao processamento automático e à transmissão de dados" – exclui, por exemplo, o armazenamento de dados.

Também, há quem prefira classificar os crimes informáticos como crimes informáticos puros e crimes informáticos impuros. Os primeiros corresponderiam aos crimes em que dados e sistemas informáticos constituem o objeto do crime. Os segundos diriam respeito aos crimes em que os recursos informáticos constituem o meio de execução, tendo como objeto bens jurídicos que já são protegidos por tipos penais existentes. Preferimos uma classificação análoga. São, basicamente, duas as espécies de crimes informáticos, os crimes informáticos comuns e os crimes informáticos específicos. Nos crimes informáticos comuns, a informática é utilizada como meio para a prática de condutas que já são consideradas crime pelo direito penal vigente. A conduta ilícita já é objeto de punição. A situação não é a mesma com os crimes informáticos específicos, em que se praticam condutas contra bens jurídicos que ainda não são objeto de tutela penal. No caso dos crimes informáticos comuns, o fato de a informática ser utilizada como meio para a prática do crime não desvirtua o tipo penal, não impede, necessariamente, que ele incida. O instrumento informático pode não ser essencial para que se cometa o crime, que poderia ser praticado por meio de outra ferramenta[14]. Com os crimes informáticos específicos, a situação é diferente. Como se praticam condutas contra bens jurídicos que ainda não são objeto de tutela, o direito penal pode não incidir, por atipicidade. O crime informático constitui uma parte de uma forma mais ampla de atividade criminosa, o crime do colarinho branco[15].

A utilização não autorizada de sistemas informáticos constitui uma conduta com uma carga de ilicitude penal muito tênue. O interesse a ser tutelado pode ser insignificante. Dificilmente, nessas circunstâncias, o direito penal tem como incidir. A situação pode ser diferente com condutas que provocam um resultado direto negativo na sociedade como um todo, se o acesso não autorizado for acompanhado da violação de segredo informático, por exemplo, a invasão do sistema informático de uma instituição financeira, com a captura de números de contas-corrente e de senhas. Dada a importância do interesse a ser tutelado, o Poder Judiciário pode recorrer à interpretação extensiva, chegando a uma fronteira próxima da analogia *in malam partem*. Ao tipificar-se o crime informático, não se deve esquecer que é preciso evitar termos técnicos em demasia, lançando-se mão apenas dos que se fizerem estritamente necessários, já que eles podem tornar-se obsoletos dentro de alguns meses, e não de anos. São várias e rápidas as modificações às quais a tecnologia da informação é submetida.

Tem-se de levar em consideração novos padrões de comportamento, que podem ser sistematizados na medida em que se analisem os interesses jurídicos colocados em risco. Uma sociedade democrática não pode correr o risco de permitir que, com base na analogia *in malem partem*, se determine o que pode e o que não pode ser objeto de sanção penal em sede de criminalidade informática. O Código Penal holandês, por exemplo, foi adaptado sistematicamente a essa nova realidade, com a criminalização de condutas tendo como objeto ataques a dados armazenados, processados ou transmitidos por sistemas informáticos. Reformularam-se artigos já existentes, adotaram-se novos artigos.

3 CARACTERÍSTICAS DO CRIME INFORMÁTICO

Os sistemas informáticos, os terminais bancários automáticos e todos os suportes de dados constituem alvos fáceis para atos ilícitos e merecem proteção especial. Os locais onde dados são coletados, armazenados, processados e transmitidos são vulneráveis. Esse problema assume uma dimensão especial quando eles são transmitidos de um sistema informático a outro, mediante redes de computadores, ultrapassando fronteiras, colocando em risco sua disponibilidade, integridade e exclusividade. A concentração de dados em sistemas informáticos interconectados pode estimular a criminalidade informática. Uma empresa pode colocar em risco sua própria existência, ao armazenar num sistema interconectado dados sensíveis ou estratégicos com relação ao desenvolvimento de novos produtos, balanços contábeis ou listas de clientes[16].

Redes de computadores e de telecomunicação eliminaram o fator distância, na prática do crime. Muitos crimes informáticos transcendem fronteiras. Vários casos podem ser mencionados. Crianças da Dalton School, em Nova York, invadiram cerca de vinte bancos de dados canadenses, incluindo arquivos de autoridades públicas. O sistema informático da Organização do Tratado do Atlântico Norte (Otan), bem como da Nasa (*National Aeronautics and Space Administration*) também já foram invadidos. A disseminação de vírus, um programa de computador que pode, freqüentemente, reproduzir-se e infectar outros softwares, apagando dados, bloqueando o funcionamento de sistemas informáticos, também se beneficia da eliminação do fator distância. O crime informático pode ser praticado em nanossegundos, não em horas, tampouco em minutos. Isso dificulta as chances de descobrir-se o responsável. Ele pode, dependendo do caso, levar anos para ser detectado. Por isso, deve-se levar a sério a adoção de medidas preventivas, de segurança. Medidas preventivas inadequadas podem, por outro lado, criar novas possibilidades para a prática do crime informático. Quando dados são armazenados num sistema, o processo técnico é, de acordo com alguns especialistas, sujeito a apenas um décimo das espécies de controle que seriam aplicadas aos mesmos dados, se eles fossem tratados manualmente. Um contrato sigiloso, ou valores, seria colocado num cofre.

Os envolvidos com crimes informáticos costumam ser divididos em duas categorias. Os profissionais e os amadores. Crimes mais sérios do que violação de segredo informático, envolvendo grandes prejuízos econômicos, são praticados por pessoas com experiência em invasão de sistemas. Muitos são empregados insatisfeitos que sabem muito bem como o sistema informático da empresa na qual trabalham funciona. Sua motivação é orientada pelo lucro, às vezes pela necessidade. Atentados contra a segurança de sistemas informáticos por empregados, geralmente, são atos de vingança. Às vezes, uma revolta contra a estrutura supostamente desumana e anti-social da empresa, um sentido de desafio, de competição. A segunda categoria, a dos amadores, compreende os jovens gênios em informática, aos quais já fizemos alusão, que aprenderam todos os truques da tecnologia da informação, incluindo como violar códigos de segurança. Podem até ajudar na detecção de falhas na segurança de sistemas informáticos. No geral, são considerados perigosos. Dados podem ser destruídos por negligência, o acesso a sistemas pode ser bloqueado, e deficiências na segurança podem ser utilizadas posteriormente com fins ilícitos.

Um grupo de *hackers* geralmente tem de três a oito integrantes de 15 a 25 anos, que não se conhecem pessoalmente. São jovens de classe média, comunicam-se via *e-mail*, *chat* ou ICQ. Muitos agem apenas

como pichadores, desfigurando as páginas para chamar atenção, mas vários se profissionalizam. A experiência como *hacker* pode ser um bom ensejo para arranjar trabalho. Empresas de segurança contratam-nos. Além de conhecer falhas em sistemas informáticos e saber como saná-las, a maioria deles pode agir, inicialmente, apenas por diversão, sem intenção criminosa. Muitas empresas, buscando mão-de-obra especializada em invasão de sites, entram em contato com *hackers* via *e-mail*. Eles, então, passam a invadir sites não mais por diversão, mas sob encomenda de concorrentes. Isso pode compreender a exigência de repasse de dados da empresa cujo site for invadido, bem como a lista completa dos seus respectivos clientes: número de carteira de identidade, endereço, o que compravam e como pagavam. O *hacker* pode ficar uma semana analisando o sistema, copiando dados de dezenas ou milhares de cadastros e, ao final, alterar os preços dos produtos oferecidos. O administrador do site pode descobrir que ele foi invadido apenas depois que a página principal for alterada. O pagamento pode ser enviado a uma caixa postal.

Como já tivemos a oportunidade de mencionar, não é fácil estimar a extensão dos crimes informáticos. Não é possível quantificar com precisão quantos crimes informáticos ocorreram num dado período no Brasil, ainda mais já que eles sequer foram tipificados. Existe também, efetivamente, uma falta de colaboração entre as vítimas e as autoridades policiais. Muitas sequer informam o ocorrido. Elas não se sentem seguras com o modo como as autoridades policiais poderão comportar-se. A polícia, de uma maneira geral, ainda não está acostumada a investigar crimes informáticos. Ela pode prejudicar o curso normal dos negócios da empresa. Apreender partes do sistema informático, bem como disquetes, pode causar um verdadeiro caos no curso dos negócios, bem como no próprio processo de produção do empreendimento. Outra razão para não levar ao conhecimento das autoridades competentes a prática de um crime informático, é que a vítima pode preferir a obtenção de uma indenização por parte do responsável, se ele puder pagá-la, a suportar os danos e processá-lo criminalmente. O número de mulheres que cometem crimes informáticos pode ser o mesmo do de homens, o que não costuma ser a regra[17].

4 OBJETOS TANGÍVEIS E INTANGÍVEIS

O direito penal enfrenta problemas ao disciplinar a criminalidade informática, já que seus fundamentos estão orientados para a proteção dos objetos tangíveis. A proteção dos objetos intangíveis já é contemplada pelo direito penal, com relação, por exemplo, aos segredos profissionais e de negócio, bem como pelo direito autoral e pelo direito das patentes, no que diz respeito, respectivamente, às obras intelectuais e invenções, mas ela não desempenhou um papel central até a segunda metade do século XX. Nas últimas décadas, a situação alterou-se profundamente. O desenvolvimento da sociedade pós-industrial, o aumento crescente do valor dos dados armazenados, processados ou transmitidos por sistemas informáticos, tanto sob o ponto de vista cultural como econômico e político, têm desafiado o direito penal. A mudança de paradigma, da tutela dos objetos tangíveis para a dos objetos intangíveis, desafia-o. Muitos objetos tangíveis têm, num crescendo, um valor de mercado inferior ao dos intangíveis.

O direito penal foi concebido tendo em vista a propriedade material, sobre objetos tangíveis. "Coisas móveis"[18] correspondem a objetos tangíveis. Em que medida dados armazenados, processados ou transmitidos por sistemas informáticos podem ser considerados coisas móveis, à luz do Código Penal? Se a resposta para tal indagação for afirmativa, então eles podem gozar da proteção conferida contra furto, roubo, dano, apropriação indébita. Objetos tangíveis e intangíveis variam consideravelmente, sob o ponto de vista jurídico. Aqueles podem pertencer exclusivamente a uma pessoa, já com estes pode ocorrer o contrário. A proteção dos objetos intangíveis tem de levar em consideração não apenas os interesses de seus titulares, mas também os interesses das pessoas a quem eles dizem respeito, tendo em vista a proteção à intimidade.

Dados armazenados, processados ou transmitidos por sistemas informáticos não podem ser considerados coisas móveis, ao contrário da energia elétrica[19], por vários fatores. Essa tem uma existência independente. Pode ser acumulada e transportada. A energia possui um valor econômico específico para a pessoa

que a gera, já que se precisa gastar dinheiro para produzi-la. Quem gera energia, pode utilizá-la para seus próprios fins, bem como transmiti-la a terceiros, tendo como contrapartida uma remuneração. Dados também poderiam ser considerados coisas móveis, de maneira análoga à energia elétrica? Eles também podem ser reproduzidos e transmitidos, bem como possuir um valor econômico específico. Se os dados armazenados, processados ou transmitidos por sistemas informáticos forem considerados coisas móveis, este conceito deixará de corresponder a objetos tangíveis para incluir objetos intangíveis. Ele passará da materialidade à imaterialidade, do âmbito da propriedade para o âmbito do valor. Essa tendência expande excessivamente o conceito de coisas móveis.

Tanto dados como coisas móveis podem ser transferidos, reproduzidos, assim como possuir valor econômico. Mas há diferenças. Coisas móveis, incluindo a eletricidade, são o produto do esforço físico, enquanto dados, do esforço mental. Estes refletem ou incorporam conhecimento. Coisas móveis são únicas. A posse de uma coisa móvel implica que outros não tenham a propriedade ou a posse da mesma coisa móvel. Dados, por outro lado, são múltiplos. A posse de dados armazenados num sistema informático não significa que outros não tenham a posse dos mesmos dados. O ato de copiar um conjunto de dados não impede que terceiros, ou o titular do próprio conjunto de dados, continue a possuí-los. O titular não perde a posse dos dados, ele perde apenas a posse exclusiva deles. Dados não podem ser considerados coisas móveis. Constituem uma categoria jurídica à parte.

Já que dados armazenados, processados ou transmitidos por sistemas informáticos não podem ser considerados coisas móveis, eles não podem ser objeto de crimes patrimoniais clássicos, como furto, roubo, dano, apropriação indébita. Dados, objetos intangíveis, não pertencem à categoria jurídica das coisas móveis, objetos tangíveis. Quando eles são copiados, os crimes patrimoniais clássicos não ocorrem. Eles podem ser objeto de crimes patrimoniais clássicos apenas quando formarem uma unidade material com o respectivo suporte. Os dados precisam estar incorporados ao suporte. Enquanto tais, eles não podem ser objeto de crimes patrimoniais. O direito penal protege o meio, o objeto tangível no qual os dados estão arquivados. O disquete onde os dados estão armazenados pode ser furtado, mas não os dados por si mesmos. Apenas objetos tangíveis podem ser objeto de furto, roubo, dano, apropriação indébita. Com o furto, subtrai-se um objeto tangível. Quando dados são "furtados", eles não são subtraídos. O titular continua na posse dos dados, mas não exclusivamente. Quem se apropria de coisa móvel, exclui outrem de sua posse. Isso não acontece com dados. Eles não obedecem a essa particularidade essencial, que tão bem caracteriza os objetos tangíveis. Quem os copia, não pode ser enquadrado por furto[20]. Essa diferenciação, sobre objetos tangíveis e intangíveis, será retomada ao longo desta obra. Tampouco o crime de falsificação diz respeito a dados, mas a documentos, objetos tangíveis, corporificados de uma maneira não transitória, duradoura. Dados armazenados, processados ou transmitidos por sistemas informáticos, que muitas vezes comprovam relações jurídicas, são objetos intangíveis, carentes dessa projeção não transitória, duradoura dos documentos[21].

5 INTERESSES JURÍDICOS

Três espécies de interesses jurídicos devem ser protegidas com relação à criminalidade informática: a disponibilidade de meios; a integridade de sistemas informáticos e de dados; e a exclusividade de meios e de dados[22].

Tanto o setor público como setor o privado dependem cada vez mais da informática. A disponibilidade de meios diz respeito ao armazenamento, processamento e transmissão de dados. O colapso de um sistema informático pode ter enormes conseqüências para uma repartição pública ou para uma empresa, bem como para a sociedade em geral. Basta pensar nas conseqüências que uma instituição bancária pode sofrer se, ainda que por algumas horas, não puder mais efetuar ordens de pagamento, ou de uma agência de viagens que não puder mais acessar a base de dados de companhias aéreas.

Com relação à integridade de sistemas informáticos e de dados, quer-se dizer que os dados e programas não devem ser corrompidos. Dados adulterados podem provocar sérias conseqüências. Processos de produção industrial, por exemplo, podem entrar em colapso. O que pode acontecer com o sistema de segurança de uma central nuclear, se os respectivos dados forem alterados, ou se dados de pacientes de hospitais forem modificados aleatoriamente? Para a obtenção de resultados corretos e para ser capaz de tomar as decisões adequadas ao utilizarem-se sistemas informáticos, torna-se extremamente importante que eles funcionem corretamente, e que seus dados e programas não sejam conspurcados. Tanto sistemas informáticos como dados devem permanecer íntegros. Qualquer disfunção pode ter conseqüências custosas, devastadoras e de grande escala para sistemas de controle de tráfego aéreo e marítimo, de geração de energia, de dosagem de medicamentos em hospitais, de pagamento. A integridade de sistemas informáticos e de dados também pode ser prejudicada com a falsificação informática.

A terceira modalidade de interesse jurídico a ser protegida, a exclusividade de meios e de dados, remete à proteção à intimidade, do segredo de dados armazenados, processados ou transmitidos por sistemas informáticos, que forem protegidos contra acesso não autorizado. Não é do interesse nem do setor público nem do setor privado que pessoas não autorizadas tenham acesso a essa espécie de dados, os quais devem manter sua natureza confidencial. Para que se mantenha esse caráter exclusivo, deseja-se ter controle sobre como os dados são utilizados e por quem. Eles não surgiram de graça, sendo o resultado de investimentos efetuados.

6 **CONCLUSÃO**

Desde 1º de agosto de 1986, foi adotada, na Alemanha, a Segunda Lei de Combate à Criminalidade Econômica (2. WiKG[23])[24]. A par de vários artigos sobre crimes econômicos, ela também contém, especificamente, artigos sobre crimes informáticos; com ênfase à projeção econômica da criminalidade informática. Em virtude da rígida aplicação do princípio da legalidade no direito penal alemão, foi preferiu, desde o princípio, encontrar uma solução para os crimes informáticos mediante a adoção de tipos penais autônomos. O Código Penal alemão, artigo 303, protege objetos tangíveis, coisas móveis, contra danos à sua substância e funcionalidade. Não protege dados contra apagamento. Estes não podem ser considerados objetos tangíveis, coisas. Enquadrar apenas o dano ao suporte no qual os dados são armazenados, não seria de grande valia. Nem sempre eles estão vinculados a tal meio, a um suporte, por exemplo – durante sua transmissão. Dados poderiam ser protegidos contra obtenção não-autorizada, sob o ponto de vista do artigo 201, referente à interceptação de comunicação, e do artigo 202, ao sigilo de correspondência, mas essa proteção teria um alcance reduzido.

O legislador alemão preferiu não criar tipos desvinculados daqueles já existentes. Adotaram-se paralelos entre o artigo 202a (espionagem de dados) e o artigo 202 (sigilo de correspondência); o artigo 263a (estelionato informático) e o artigo 263 (estelionato); o artigo 269 (falsificação de dados juridicamente relevantes) e o artigo 267 (falsificação de documentos); o artigo 303a (dano informático) e o artigo 303 (dano). Aprovou-se uma dupla tipificação, para evitar dúvidas sobre a incidência do direito penal com respeito à criminalidade informática. A fraude de dados para fins de estelionato é enquadrada pelo artigo 263a e pelo artigo 303a do Código Penal. O mesmo pode ser dito da fraude de dados tendo em vista sua falsificação (artigo 269 e artigo 303a) e da manipulação de dados com fins de atentado contra a segurança de sistema informático (artigo 303b e artigo 303a).

O direito penal holandês, baseado originariamente no Código Penal napoleônico, sofreu influências tanto da doutrina alemã como da francesa. A Lei de Criminalidade Informática[25] entrou em vigor nos Países Baixos em 1º de março de 1993. Ela sofreu influência do direito alemão. A Segunda Lei de Combate à Criminalidade Econômica antecedeu-a em quase sete anos. O legislador holandês, à semelhança de seu colega alemão, também concluiu que o Código Penal de seu país dificilmente poderia ir de encontro à criminalidade informática, por motivos que já foram analisados anteriormente. O Código pre-

vê o furto, apropriação indébita e dano com relação à "subtração", "apropriação" e "dano" de um bem[26], de coisas móveis. Dados armazenados, processados ou transmitidos por sistemas informáticos não podem ser considerados coisas móveis, tampouco, necessariamente, têm valor econômico. Eles tampouco poderiam ser considerados, pacificamente, documentos[27], à luz do artigo 225 do Código Penal. Documentos, para o direito penal holandês, embora não precisem ser diretamente legíveis pelo ser humano, precisam ter uma forma durável, não volátil.

Foram acrescentadas duas novas definições jurídicas ao Código Penal holandês, a de dados ("*gegevens*") e de mecanismo automatizado ("*geautomatiseerd werk*"). O primeiro termo foi adicionado para que, explicitamente, ficasse claro que dados não poderiam ser considerados coisas móveis. Mecanismos automatizados são os dispositivos cujo funcionamento independe de intervenção humana. Abrange, essa definição, por exemplo, sistemas informáticos, redes de computadores e instalações automatizadas de telecomunicação. Não compreende relógios etc. O *hacking*, o acesso não autorizado a sistemas informáticos protegidos, foi tipificado (artigo 138a). Tanto o acesso não autorizado externo, efetuado via internet, quanto o acesso não-autorizado interno, mediante intranet, são objeto de sanção penal. Basta que uma medida de segurança qualquer seja violada.

O Código Penal holandês protege não apenas dados enquanto tais, no caso de dano informático (artigos 350a-350b), bem como o meio através do qual os dados circulam, as redes de telecomunicação[28]. Não são, agora, os dados, o objeto intangível, que são protegidos, mas o meio tangível mediante o qual os dados trafegam. O conceito da livre circulação de informação desempenha, nesse aspecto, um papel importante. O princípio é que dados, ao contrário das coisas móveis, cuja proteção é orientada pelo princípio da propriedade, devem circular livremente. Para tanto, os meios através dos quais eles transitam devem gozar de proteção específica. Considerando insuficientes conceitos clássicos como "destruição" e "deterioração", o legislador holandês adotou os artigos 350a-350b, para oferecer proteção contra quem modificar, apagar, inutilizar ou tornar inacessíveis dados armazenados, processados ou transmitidos por computador. Quem disseminar vírus, também pode ser enquadrado com base em tais artigos.

O Brasil, à semelhança da Alemanha e dos Países Baixos, deve reformar sua legislação penal, adaptando-a à proteção dos bens intangíveis na era da criminalidade informática.

Intangible Objects in the Computer Crime Age

Abstract

This article analyzes the protection of intangible objects in terms of computer crime, based upon the German law and the Dutch law. The article delineates the concept of computer crime, distinguishing its main characteristics. By differentiating tangible objects from intangible objects, the article defends the criminal law reform founded on legal interests which deserve specific protection.
Keywords: Tangible objects. Crime. Criminality. Computer.

Notas explicativas

[1] Lei nº 9.507, de 12 de novembro de 1997 Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

[2] Constituição Federal, artigo 5º, inciso LXXII: "Conceder-se-á *habeas data*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

[3] Lei nº 9.983, de 14 de julho de 2000 Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.
[4] Ressaltem-se outras inovações legislativas no âmbito da informática: Decreto nº 3.505, de 13 de junho de 2000 Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; e Decreto nº 3.587, de 5 de setembro de 2000 Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências.
[5] Lei nº 9.609, de 19 de fevereiro de 1998 Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
[6] Desde 17 de agosto de 1991, Portugal tem sua própria legislação sobre crimes informáticos, a Lei nº 109/91. À semelhança de seus congêneres europeus, ela oferece proteção contra: falsidade informática (artigo 4º); dano relativo a dados ou programas informáticos (artigo 5º); sabotagem informática (artigo 6º); acesso ilegítimo (artigo 7º); interceptação ilegítima (artigo 8º); e reprodução ilegítima de programa protegido (artigo 9º).
[7] O Computer Misuse Act data de 1990.
[8] A telemática é a ciência que trata da manipulação e utilização da informação através do uso combinado de computador e meios de telecomunicação.
[9] O medo do desemprego talvez seja o maior deles.
[10] A criminalidade informática.
[11] Talvez um dos argumentos mais fortes para a modernização do direito penal seja a existência de novas modalidades criminosas que merecem sanção penal. Por exemplo, o *hacking*.
[12] Computer-related Crime (Recommendation nº R 89(9)). Strasbourg, Council of Europe, 1990, p. 13.
[13] *Ibidem*, p. 13.
[14] Por exemplo, em sede de crimes contra a honra.
[15] Computer-related Crime (Recommendation nº R 89(9)). Strasbourg, Council of Europe, 1990, p. 18.
[16] Bancos de dados geralmente contêm um volume considerável de informação com projeção econômica.
[17] FRANKEN, Hans. Computing and Security. In: *Amongst Friends in Computers and Law*. Ed. H.W.K. Kaspersen e A. Oskamp. Deventer/ Boston: Kluwer Law and Taxation Publishers, 1990, p. 132.
[18] Código Penal, artigo 155, caput.
[19] *Ibidem*, artigo 155, § 3º.
[20] O legislador holandês decidiu não subsumir dados à categoria de "coisas móveis". Criou-se uma nova categoria jurídica, no artigo 80quinquies do Código Penal, a de dados, que também engloba os programas de computador. Sistemas informáticos foram definidos no artigo 80sexies. O Código Penal daquele país, artigos 350a-b, protege não apenas dados enquanto tais, no caso de dano informático ("*gegevensaantasting*"), bem como o meio através do qual os dados circulam, os serviços de telecomunicação. Nesse caso, não são os dados, o objeto intangível, que são protegidos, mas o meio tangível mediante o qual os dados trafegam.
[21] O conceito da livre circulação de informação desempenha um papel importante na proteção dos objetos intangíveis. O princípio é que dados, ao contrário das coisas móveis, cuja proteção é orientada pelo princípio da propriedade, devem circular livremente.
[22] Podem-se mencionar como exemplos, não exaustivos, de crimes contra a disponibilidade de meios – o atentado contra a segurança de sistemas informáticos; de crimes contra a integridade de sistemas e de dados - o dano informático, com a manipulação de dados e a disseminação de vírus, e o estelionato informático; e de crimes contra a exclusividade de meios e de dados – a violação de segredo informático.
[23] Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität.
[24] Na Áustria, a Lei de Reforma do Código Penal, de 22 de dezembro de 1987, também inseriu no Código Penal daquele país artigos contra a criminalidade informática.
[25] Wet computercriminaliteit.
[26] *Goed*.
[27] *Geschrift*.
[28] Redes de telecomunicação são os meios que proporcionam o transporte de imagens, impulsos, informação, sinais, sons, o complexo de medidas e mecanismos que tornam a comunicação possível entre pessoas a certa distância, através de sistemas informáticos, telefone, telégrafo, telex.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Ed. Juarez de Oliveira, 2006.

ALEMANHA. Deutscher Bundestag. 10. Wahlperiode. Gesetzentwurf der Bundesregierung. Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität (2. WiKG). Drucksache 10/318. 26 Aug. 1983.

BINDER, Jörg. Computerkriminalität und Dantenfernübertragung (I). **Recht der Datenverarbeitung**, Frechen-Königsdorf, v. 11, n. 2, p. 57-60, 1995.

_____. Computerkriminalität und Dantenfernübertragung (II). **Recht der Datenverarbeitung**, Frechen-Königsdorf, v. 11, n. 3, p. 116-123, 1995.

BOXTEL, C. van. Nieuwe wetgeving voor de elektronische snelweg. **Bedrijfsjuridische berichten**, Zwolle, n. 10, p. 99-101, 13 mei 1998.

_____. Computer-related Crime (Recommendation nº R 89(9)). Strasbourg, Council of Europe, 1990.

CONINCK, Christian de. Computermisdrijven: een onderschatte criminaliteit. **Politiejournaal en Politieofficier**: het Belgisch politievakblad, Bruxelas, n. 7, p. 13-18, 1991.

CORSTENS, G. J. M. Internet en strafrecht: bespreking van het preadvies van Y. Buruma, "Internet en strafrecht". **Nederlands Juristenblad**, s.l., v. 73, n. 23, p. 1032-1035, 5 juni 1998.

DANNECKER, Gerhard. Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung. **Betriebsberater**, Heidelberg, v. 51, n. 25, p. 1285-1294, 20 Juni 1996.

DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Cybercrimes. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & internet** – aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. p. 117-129.

DERKSEN, Roland. Die Hinterlegung einer Anleitung zur Herstellung von Sprengstoffen in einer Mailbox – ein strafbarer Verstoss gegen das Waffengesetz? **Neue Juristische Wochenschrift**, Munique, v. 51, n. 51, p. 3760-3761, 1998.

DIJK, Chr. H. van; Keltjens, J. M. J. **Computercriminalteit**. Zwolle: W.E.J. Tjeenk Willink., 1995.

DOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato Opice (Coord.). **Direito eletrônico**: a internet e os tribunais. Bauru: EDIPRO, 2001. p. 203-221.

ENKELENS, C. Beteugeling van computercriminaliteit: een terreinverkening. **Panopticon**, Bruxelas, p. 334-345, 1985.

FERREIRA, Ivette Senise. A intimidade e o direito penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 2, n. 5, p. 96-106, jan./mar. 1994.

FRANKEN, Hans. Computing and Security. In: KASPERSEN, H. W. K.; OSKAMP, A. (Ed.). **Amongst Friends in Computers and Law**. Deventer/Boston: Kluwer Law and Taxation Publishers, 1990, p. 131-140.

GOUBERT, Luc. Computerfraude. **Tijdschrift voor Accountancy en Bedrijfskunde**, Bruxelas, v. 14, n. 2, p. 61-67, 1989.

GROENHUIJSEN, M. S. Criteria voor strafbaarstelling. **Delikt en delinkwent**, Deventer, v. 23, n. 1, p. 61-67, 1993.

JAEGER, Stefan. Anbieten von "Hacker-Tools" – Zur Strafbarkeit "neutraler Handlungen" als Beihilfe. **Recht der Datenverarbeitung**, Frechen-Königsdorf, v. 14, n. 6, p. 252-255, 1998.

_____. **Computerkriminalität**. 2. Ed. Augsburg: Interest-Verlag, 1998.

KASPERSEN, H. W. K. De wet computercriminaliteit is er – nu de boeven nog. **Computererecht**, Deventer, n. 4, p. 134-145, 1993.

KOOPS, Bert-Jaap; SCHELLEKENS, M. H. M. Computercriminaliteit II: de boeven zijn er – nu de wet weer. **Nederlands Juristenblad**, s.l., v. 74, n. 37, p. 1764-1772, 1999.

_____. Het Cybercrime-verdrag, de Nederlandse strafwetgeving en de (computer) criminalisering van de maatschappij. **Computerrecht**, Deventer, n. 2, p. 115-123, 2003.

MÖHRENSCHLAGER, Manfred. Das neue Computerstrafrecht. **Zeitschrift für Wirtschafts- und Steuerstrafrecht**, Heidelberg, n. 4, p. 128-142, 1986.

RAHAL, Flávia; GARCIA, Roberto Soares. Crimes e internet: breves notas aos crimes praticados por meio da rede mundial e outras considerações. **Boletim IBCCRIM**, São Paulo, v. 9, n. 110, p. 8-9, jan. 2002.

REIS, Maria Helena Junqueira. **Computer crimes**: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1997.

ROOS, Theo de. Het concept-wetsvoorstel computercriminaliteit II. **Computerrecht**, Deventer, n. 2, p. 55-58, 1998.

ROOS, Theo de; KOOPS, Bert-Jaap; DIJK, Chris van. Materieel strafrecht en ICT. Eds. J.E.J Prins a. o. In: **Recht & Informatietechnologie**. A Haia: Sdu, s.d., p. 9.3/1-9.3/39.

SCHMID, Niklaus. Die neuen Computerstraftatbestände. **Diritto penale economico, atti della giornata di studio del 14 ottobre 1996**. Lugano: Commissione ticinese per la formazione permanente dei giuristi, p. 41-66, 1999.

SCHUIJT, Gerard. Wet computercriminaliteit II: van uitgever en drukker naar tussenpersoon. **Mediaforum**, s.l., v. 10, n. 3, p. 70-75, 1998.

SIEBER, Ulrich. Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1). **Juristen Zeitung**, Tübingen, v. 51, n. 9, p. 429-442, 1996.

_____. Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2). **Juristen Zeitung**, Tübingen, v. 51, n. 10, p. 494-507, 1996.

_____. The Emergence of Criminal Information Law. In: KASPERSEN, H. W. K.; OSKAMP; A. (Ed.). **Amongst Friends in Computers and Law**. Deventer/Boston: Kluwer Law and Taxation Publishers, 1990, p. 117-129.

VIANNA, Túlio Lima. Dos crimes pela internet. **Revista do CAAP**, Belo Horizonte, v. 5, n. 9, p. 367-385, 2000.