ASPECTOS PENAIS DOS CRIMES DE INFORMÁTICA NO BRASIL

OTTO BANHO LICKS
e
JOÃO MARCELLO DE ARAÚJO JÚNIOR

"Les temps modernes sont souvent, dans les pays hautement industrialisés, caratérisés par le terme de révolution informatique. Le tempo que précèdent, à partir de la moitié du siècle passé, se viot, de son côté, caratérisé par la notion de révolution industrialle, le développement presque explisif, et l'usage répandu, des machines.[1]

1. Introdução

Os avanços tecnológicos têm mudado a história do mundo e tranformado a sociedade. A invenção da Imprensa, a descoberta da eletricidade, a invenção do telefone e do automóvel, por exemplo, causaram uma fundamental redefinição do comportamento social, político, comercial e militar.

Durante a segunda metade deste século, testemunhamos dois dos mais profundos avanços tecnológicos: a evolução e a disseminação do uso dos computadores. Há dez ou doze anos atrás, uma verdadeira revolução ocorreu, quando os micro-computadores começaram a se tornar comuns. Agora, uma outra revolução, indiscutivelmente maior do que a primeira, está acontecendo. É o advento das redes de computadores.[2]

A rapidez e a irreversibilidade destas mudanças acabaram gerando o que se convencionou chamar de revolução da informação, e, que Bell definiu como sociedade pós-industrial. Diante desse fato, devemos dizer, preliminarmente, que não temos que considerar os crimes por computador, como o preço do progresso. Para protegermos a nós mesmos e aos nossos computadores, precisamos substituir os mitos do passado pela realidade do

1. "Os tempos modernos são freqüentemente, nos países altamente industrializados, caracterizados pelo termo de revolução informática. Os tempos que precedem a partir da metade do século passado, vêem-se, de sua forma, caracterizados pela noção de revolução industrial, tendo em vista o desenvolvimento explosivo, e o uso corrente das máquinas" Klaus Tiedemann, *Ciência e Política Criminal em Honra de Heleno Fragoso*, Organizador Prof. João Marcello de Araujo Junior, Grupo Brasileiro da Associação Internacional de Direito Penal, Forense, Rio, 1992.

2. Ver E. de Krol, *The hole internet catalog & user's guide*, O'Relly & Associates, 1992

presente. A noção ou a falsa idéia de que o crime por computador é um problema relacionado com técnicos de informática, segundo BloomBecker, seria o pior deles.[3]

A mudança sofrida pela sociedade, advinda dos avanços tecnológicos, trouxe como conseqüência previsível e mediata a transformação do Direito e das relações jurídicas também. Hoje, somos forçados a reajustar o Direito, em especial o Direito Criminal, pra adaptá-lo às novas condutas criminosas.

Este estudo visa abordar o atual estágio dos institutos relacionados com os crimes por computador. Serão analisados os conceitos e definições desses crimes à luz da doutrina interna e internacional. Também serão indicadas e discutidas as soluções já adotadas por outras legislações para lidar com este tipo de criminalidade, cada vez mais presente em nossa sociedade.

A análise a que nos propomos, tem por objetivo sugerir, a partir do estudo crítico do que já existe na legislação comparada, os elementos teóricos que deverão nortear a reforma do direito penal brasileiro, no capítulo relativo aos crimes de informática, uma vez que tal tema jamais foi tratado de forma sistemática pela doutrina pátria.

As pesquisas apresentadas neste trabalho seguem três campos de estudos. No primeiro, trataremos das áreas específicas do Direito Penal relacionados com a Informática, tal como a definição dos seus termos. Em seguida, estudaremos a teoria geral do Direito Penal aplicado aos crimes por computador. Por último, analisaremos os institutos jurídicos que tangenciam o direito criminal, como o direito do autor, a proteção à intimidade e aos segredos de indústria e de comércio.

Todos esses temas serão considerados em tópicos separados. Um deles será dedicado ao estudo das transformações do direito penal positivo em decorrência das situações geradas pela sociedade informatizada. A atual legislação brasileira será discutida e a proposta de anteprojeto da nova parte especial do código penal brasileiro apresentada.

2. Direito da informática como disciplina autônoma

O ajustamento do Direito à sociedade informatizada, antes de particularizar-se no Direito Criminal, passa por uma visão mais geral. Esta forma especial de tecnologia, deu surgimento a um novo ramo do direito, denominado *information law, Computer law* ou Direito de Informática. Outros avanços tecnológicos.

Entretanto não tiveram o mesmo impacto sobre o Direito. Maggs, Soma e Sprowl[4] trazem algumas considerações que achamos interessantes reproduzir:

"Is there a subject as "computer law?" If so, shat should a computer law casebook include? The answers to these questions are not obvious. Certainly there are many cases involving computers. A recent Westlaw search for the word "Computer" found 11,288 cases in the "allfeds" dada base and

3. Buck BloomBecker, *Spetacular Computer Crimes*, Dow Jones-Irwin, Homewood, Illinois, 1990.

4. Peter B. Maggs, John T. Soma, James A. Sprowl, *Computer Law — Cases Comments — Questions*, West Publishing Co., U.S.A., 1992, p. 1.

8,928 cases in "allstates". A similar search for "Shoe" found 15,867 Federal and 25,104 state "Show" cases. No one os suggesting that law students should study "shoe law" as a separete course. Students will read Brown Shoe Co. v. United States, 370 U.S. 294 (1962), a leading vertical mergeg case, in their antitrust course. Little or nothing in these cases turns on anything peculiar about shoes. Cases involving shoes do not cite other cases involving shoes. Computer cases, in contrast, often turn on the special nature of computer software and hardware, and regulary cite other computer cases.

Why are computer "special" when shoes are hot? First, computer software and hardware are the most complex and rapidly developing intellectual criations of modern man. Second computers provide umprecedent power in accessing and manipulating data. Third, computers work in complex systems that require standarization and compatibility to function".[5]

Poderiamos ir mais além, dizendo mesmo, que a sociedade pós-industrial informatizada tornou-se dependente dessa tecnologia, sendo essa dependência a que faz o computador tão especial.[6]

Essa dependência manifesta-se de forma inquestionável, por exemplo, com os inúmeros EFT (Eletronic Founds Transfer), realizados, diariamente, com o trabalho da SWITF (Society for World-wide Interbank Financial Telecomunications), ou da ACESS (American Computerized Ciomodity Exchange System and Services), ou, mais especificamente no Brasil, através de sistemas como o SISBACEN (do Banco Central), ou o SISCOMEX, (do Departamento de Comércio Exterior do Ministério da Economia), sem falar nos outros diversos tipos de EDI (Eletronic Data Interchange), a tal ponto que as relações entre a informatização e os seus reflexos no direito deram lugar àquilo que o Prof. Ulrich Sieber[7] chamou de Ius Informationis.

Para se ter uma idéia da dimensão da utilização dos computadores, a Secretaria de Fazenda do Estado de São Paulo espera que num futuro próximo 70% da arrecadação do Estado seja proveniente de contribuintes que utilizam sistemas de computadores para a escrituração fiscal, contábil e, para a emissão de notas fiscais a laser. Os contribuintes que optarem por esse sistema informatizado de escrituração fiscal estarão dispensados de todos os documentos fiscais.

5. Ib. id. p. 1

6. Do *United Nations Manual on Computer-Related Crimes (draft) for discussion at the United Nations "Ad Hoc" Meeting of Experts Wurzburg*, Germany, 1992, à p. 1, podemos retirar a seguinte citação: "Information technology today touches every aspect of life, irrespective of location on the globe. Our dally activities are affected in form, content and time by the computer. Business, governments and individuals all have and continue to recelve the benefits of this information revolution. While providing tangible benefits in time and money, the computer has also had impact on everyday life, as computerized routines replace mundane human task. More and more of our business, industries, economies, hospitals and governments are becoming dependent upon computers". Tal é também o entendimento do Conselho da Europa. Computer-Related Crime: Recommendation No. R (89)9 on computer-related crime and final report of the European Committes on Crime Problems (Strasbourg, 1989).

7. Ulrich Sieber, *The International Emergence of Criminal Information Law*, Carl Heymanns Verlag KG, Germany, 1992.

O estudo do direito criminal de informática, assim como do direito de informática, abrange, ao nosso ver, diversos ramos de estudos. Não vamos tratar dos crimes já tipificados cometidos com o emprego de sistemas de computadores, nem da proteção da privacidade, e, nem dos modos de produção de prova, embora constituam importantes áreas de estudos. Ficaremos restritos aos fundamentos dos crimes de informática ditos "puros", ou seja, dos novos tipos advindos da sociedade pós-industrial. Falaremos destas outras áreas de estudo, de maneira tangencial quando da análise do projeto da parte especial do código penal.

3. Alguns aspectos da teoria geral do Direito Penal e a origem dos crimes de informática em outros países

Como já foi dito, o campo da informatização da sociedade é extremamente fértil para a prática de delitos. Os atuais estudos sobre os crimes de informática estão refletindo, de maneira muito veemente, a grande preocupação e a indignação da comunidade internacional com a dependência dos computadores sofrida pela sociedade informatizada. Isto, entretanto, conduz a exageros de criminalização.

Tal preocupação parece ter trazido de volta o período inquisitivo por que passou o mundo ocidental cristão. Definições de crime de informática como *any illegal, unethical, or unauthourized behavior involving automatic data-processing and/or trnasmission of data*[8] nos levam a renegar certas garantias individuais básicas, pilares da maioria dos Estados e da comunidade internacional. O mais interessante é que, em nome dessas mesmas garantias, o próprio direito criminal de informática preocupa-se com valores fundamentais como a privacidade do indivíduo.

Preliminarmente, podemos dizer que preferimos um entendimento mais restrito dos crimes de informática.

Taber[9], ainda que de forma imprecisa, no início dos anos 80, definia crimes de informática como sendo "a crime that, in fact, occurred and in which a computer was directly and significantly instrumental". A contribuição de Taber ao Direito Criminal de Informática, ainda que não jurídica, foi relevante, visto que, de uma forma muito pragmática, acabou por influenciar juristas e pesquisadores como Parker. Foi ele o primeiro a restringir e dimensionar o alcance dos atos que poderiam ser definidos por crimes de informática. Daí, Parker[10] ter diferenciado, logo após, *Computer Crime* do que ele passou a chamar de *Computer Abuse*. Esse seria, segundo ele, "any intentional act associated in any way with computers where a victim suffered,

8. Ulrich Sieber, *The international handbook on computer crime. Computer-related Economic Crime and the infringements of Privacy, 1986, (chapter I, note 1), p. 1 et seq.*

9. John Taber, *A Survey of Computer Crime Studies*, 2 Comp. L. J. 275 (1980). BloomBecker, em seu livro *Spetacular Computer Crimes*, op. cit., p. 67, define a contribuição de Taber do seguinte modo: "Taber returned to the obscrutity in which he had previously lurked. In two very influential law review articies, and in testimony before Congress, this IBM programmes, threw down the gautiet to all those people who argued that computer crime was a serious problem requiring legislative attention."

10. Donn Parker, *Fighting Computer Crime*, capítulo 2.

or could have suffered a loss, and a perpetrator made, or could have made, a gain" enquanto *Computer Crime*, seria "...any act as specified in a computer crime statute in the applicable jurisdiction of the statute".

Podemos então dizer que, destes estudos preliminares, desenvolvidos de forma empírica, surgiram, nos EEUU os fundamentos e princípios do que chamamos de Direito Criminal de Informática e dos Crimes de Informática, que serão analisados a seguir.

3.2 Crimes de Informática e a evolução legislativa

A sociedade pós-industrial informatizada trouxe fatos novos que não encontraram abrigo nas leis penais, fruto do desenvolvimento e aparelhamento daquele estágio da ciência criminal, principalmente quando levamos em conta o positivismo e o estrito apego a tipificação das condutas exigidas pelo direito penal. Estes novos fatos podem hoje ser chamados de Crimes de Informática. Porém, isto não é o que, necessariamente, ocorre com todo e qualquer comportamento ou ação tomada neste meio informático ou tecnológico. A própria resolução proposta pelo Canadá, e que foi aceita no plano internacional pelo oitavo congresso da ONU[11] sobre crimes de informática, traz:

"...the resolution urges Member Stats to intensify their efforts to combat computer crime by:

1) modernizing national criminal laws, including the institution of measures to:

a) ensure that existing laws adequately apply to the commission of such offences when committed within the computer environment;

b) create new offences where required;"

Esta dicotomia entre o adequar as leis existentes e o criar novos tipos é, ao nosso ver, a base da diferença entre o Crime de Informática e o *computer misuse*.

Segundo Wasik,[12] na Inglaterra defendia-se, no início dos anos 80, que o meio de cometimento de um delito não requer, pelo menos em princípio, uma reforma no direito substantivo, nem uma modernização processual. Esta foi a posição do Japão até a reforma de seu Código Penal em 1987, que usava a analogia e aumentava o alcance de certos dispositivos.[13] Entretanto, está se tornando amplamente aceito na maioria dos países, que o direito penal tradicional necessita de uma urgente adequação a estes novos métodos e a estes novos fatos.[14]

11. United Nations, ECOSOC, proposals for concerted international action against forms of crime identified in the Milan Plan of Action, UN Doc. E/AC. 57/1988/16, April, 14, 1988, para. 42-44.

12. Martin Wasik, *Crime and the Computer*, Clearendon Press Oxford, Oxford, 1991.

13. Atsushi Yamaguchi, "Computer Crimes and other Crimes against information Tecnology in Japan — National Report", *International Review of Penal Law*, France, Erès, 1993, p. 437.

14. O Manual da ONU sobre crimes relacionados com o computador, a recomendação r(89)9 da Comunidade Européia e diversas leis nacionais, surgida após 1976, são um exemplo desta tendência.

A sociedade internacional começou a perceber, no decorrer dos anos 80, que o direito penal tradicional apresentava-se inadequado para lidar com certas formas de abusos,[15] na utilização dos computadores. Daí, termos assistido ao surgimento, nos países ditos mais desenvolvidos, de legislações específicas em resposta à esta carência ou inadaptação do direito penal tradicional. Porém, esta resposta, na forma de leis específicas contra os crimes por computador pecou por falta de uniformidade, tendo ainda, um vício mais grave.

Vício este que se caracterizou por tutelar os novos fatos próprios dos ambientes tecnológico da informática digital e da informatização da sociedade com os mesmos princípios de direito penal aplicáveis ao delitos corpóreos ou tangíveis. Porém, para citarmos uma diferença entre as novas situações e a utilização destes princípios, podemos dizer que, nos delitos contra bens corpóreos, as leis da física apóiam e relacionam-se com as leis criminais. O mesmo não pode ser dito quando nos referimos aos crimes de informática. Este fenômeno trará então, outros conceitos para lidar com estes novos atos e condutas merecedoras de reprovação máxima.

3.3 Crimes de Informática e dicotomia de enfoques

O que hoje se convencionou chamar de *Criminal Information Law* ou Direito Criminal de Informática, denominação que apareceu em torno da doutrina do Prof. Ulrich Sieber, é, sem dúvida, um novo ramo do direito, que possui uma dicotomia de enfoques.

De um lado tem-se a primeira posição, dos que consideram o crime de informática como outro crime qualquer, perfeitamente tipificável em face da atual legislação criminal. Para estes não há necessidade, por exemplo, de discutir-se entre a tutela garantidora da informação contida em um documento qualquer e informação contida em um computador. O computador seria apenas um instrumento facilitador na prática de um crime já previsto anteriormente pela lei penal. Por essa via, basta adaptar a lei existente ao caso concreto. O segundo grupo 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 nova legislação para combater o problema.

A pergunta que agora se coloca é se os diversos ordenamentos jurídicos, de fato, conseguiram equacionar a questão a respeito da existência de crimes próprios de informática ou da utilização dos tipos já existentes, já que no Brasil, por ora, este é o momento de tomar essas decisões para o anteprojeto de lei penal que se discute.

Com esse objetivo em mente, entendemos que, o advento da sociedade informatizada trouxe bens jurídicos novos. Além disso, deu uma nova dimensão à vários já existentes. Porém, é preciso observar o enquadramento legal das condutas que já estão abrigadas pelos dispositivos existentes. Não será o meio de perpetrar o crime, que definirá a conduta. Nem será o *nomen iuris* que conseguirá qualificar condutas tão sedimentadas em tipos já

15. Entendemos por abuso a conduta anti-ética, merecedora de reprovação máxima face aos valores da sociedade e ao sistema penal vigente.

descritos. Como Shaekespeare já escreveu: "What's in a nome? that shich we call a rose by any other name would smell as sweet."

Entendemos, como a ONU, que "Computer systems offer some new and hightly sophisticated opportunities for law-breaking, as well as creating the potential to commit traditional types of crimes in non-traditional ways"; já que certas condutas estão descritas dentro dos tipos tradicionais existentes, como por exemplo, no caso de cópias ilegais de *softwares* que são protegidos pela propriedade intelectual. Como a violação dos Direitos Intelectuais já constitui crime[16], o computador seria apenas instrumento para a perpetração deste. Apenas algumas condutas então carecem de definição e, conseqüentemente, de um novo dispositivo legal, que as tipifique, como a violação de sistema (*hacking*). Isto se deve, principalmente, porque na aplicação das doutrinas do direito penal tradicional, a exigência da tangibilidade têm sido um impedimento para punir certos crimes por computador. Por exemplo, no crime de invasão de estabelecimento industrial ou comercial, ou ainda de domicílio,[17] pressupõe-se que o agente fisicamente entre no recinto. Assim, num crime de computador, no qual o agente obtenha acesso (entre) no sistema de outro, não poderíamos utilizar a figura penal acima porque não se poderia tipificar a entrada do agente através do computador, sob pena de analogia *in mala partem*. Por isso, há necessidade de tipificar este acesso num novo tipo penal. Outro exemplo, é o do crime de furto de dados e informações, onde a agente "furta" apenas copiando, ou seja, não retira, não subtrai da esfera patrimonial do ofendido estes dados e informações furtadas. Para tipificarmos o furto, utilizando-se de definição legal, seria necessário também que o agente apagasse os dados e informações do computador do ofendido, o que já configuraria outra infração, analogicamente comparável ao dano. Daí, em nossa opinião, e, respeito ao princípio da legalidade, ser preferível a criação de novos tipos ao invés de deixar a analogia e a interpretação extensiva serem utilizadas para tentar abranger certas condutas.

Diante do exposto e, utilizando do subsídio da pesquisa da legislação comparada, com vista a uma contribuição para a parte especial do anteprojeto, no capítulo dos crime de informática, concluímos que a melhor opção é a da tipificação de quatro delitos de informática ditos "puros", ou verdadeiros Crimes de Informática, prevendo ainda outros dois dispositivos para adequação das normas penais vigentes à realidade da informática e, duas normas específicas de proteção da privacidade contra a prática de atos de atentado, especialmente graves à mesma, através do computador.

3.4 Dos Objetivos dos Crimes de Informática

Antes de entrar na definição das condutas típicas dos crimes de informática, e, antes de passarmos a descrever quais os bens jurídicos cuja proteção devem ser objeto de proteção através de ordenamento vigente, ou através de novos tipos específicos sobre os crimes de informática, começare-

16. Artigo 184 do Código Penal, com as últimas alterações introduzidas pela Lei 8.635 de 16.3.93 e, a atual Lei do "Software", Lei 7.646/87 em seu título VII.

17. Respectivamente arts. 202 e 150 do Código Penal.

mos pela questão que entendemos mais central, ou seja o objetivo do Direito Criminal de Informática.

Existe ainda hoje uma bipolarização em torno do que seja o bem jurídico fundamental protegido pelo Direito Criminal de Informática, se os sistemas de computador ou se as informações. Existem posições claras, como a do Prof. Sieber, na Alemanha, ou de Parker nos EEUU, à favor da proteção da informação, embasada na redefinição da importância das informações na sociedade pós-industrial.

O National Center for Computer Crime Data dos EEUU, por sua vez, defende a posição de que o Direito Criminal de Informática é concebido para proteger os sistemas de computadores e de comunicações, além da informação[18]. Esta seria, *prima facie* a nossa posição, muito embora não tão extremada à ponto de considerar, por exemplo a destruição física de um computador como um crime de informática, como sugere BloomBecker.[19]

Entendemos que a preocupação do Direito Criminal de Informática com os sistemas de computadores e de comunicação deve-se, fundamentalmente, à proteção dos seus componentes imateriais ou intangíveis, ou seja, o *software* e os "dados", que ainda não contam com a mesma proteção do outro componente, o *hardware* e, principalmente do que chamaremos de recurso disponível, proveniente da utilização dos sistemas de computadores em redes de computadores.

Salientamos que quando nos referimos a proteção do *software* ou dos recursos das redes de computadores não estamos nos referindo à proteção da propriedade intelectual pelo Direito, mas sim da proteção de tais bens jurídicos de todas as outras formas que não a pirataria, a cópia não autorizada, ou a contrafação. Isto porque, em nosso entendimento, a cópia não autorizada, a contrafação ou a pirataria de programas de computadores já estão reguladas pela tutela penal. No caso da legislação brasileira, pela Lei do Software, Lei 7.646/87, pela Lei dos Direitos do Autor, Lei 5.988/73 e, pelo Código Penal. Esta também é o entendimento na Holanda, onde a pirataria de *software* não é considerada como Crime de Informática.[20]

Embora a distinção entre o *hardware* e o *software* seja pacífica do ponto de vista técnico e fático, não podemos dizer o mesmo quanto às implicações jurídicas. O Direito ainda caminha lentamente para a implementação de um sistema jurídico que proteja os bens incorpóreos e imateriais tão tem quanto os bens materiais. Com isso, concordamos com as assertivas do Prof. Davis,[21]

18. Segundo o Prof. Dr. Atusushi Yamaguchi da Universidade de Tóquio. A Agência nacional de polícia japonesa define crime de informática como sendo crimes "including negligent acts or accidents *which obstruci the function of a computer system or use it illegaly*". *International Review of Penal Law*, "Computer Crime and Other Crimes Against Information Technology", Erès, 1993, p. 433 (grifos nossos).

19. BloomBecker, op. cit., p. 71

20. Henrik W. K. Kaspen, "Computer crimes ando other crimes ainst Information Technology in the Netherlands" *International Reviewof Penal Law*, France, 1993, Erès, p. 474.

21. Randall Davis, "Intellectual Property and Software: The Assumptions are Broken", in WIPO Worldwide Symposium on the intellectual property aspects artifical intelligence, Stanford University, Standford (California), EEUU, Março de 1991, publicado em Genebra em 1991.

que sustenta semelhante posição ao tratar da proteção jurídica da propriedade intelectual no âmbito da inteligência artificial, e, que achamos interessante transcrever;

"As computer scientists learn early in their education, hardware and software are assentially interchangeble. More precisely, they are what we might call behaviorally Interchangeable; any behavior we can accomplish with one we can also accomplish with the other...

If hardware and softsare are behaviorally interchangeable, the choice of which to use in any given circumstance becomes what is termed an "engineering decision"...

While ardware and software are interchangeable in the tecnical world, notice the anormous difference in the variety of intellectual property protection available depending on which of those we choose..."

3.5 Da diferenciação dos institutos existentes

Quando cogita-se da proteção de bens imateriais, temos logo o exemplo da propriedade intelectual, como o Direito do Autor, um dos mais antigos dispositivos de proteção da propriedade imaterial, que visa dar proteção ao autor de uma obra.

O Prof. Santos,[22] em seu livro, explica as teorias que justificam o Direito Autoral. Segundo ele, uma destas teorias é a dos bens jurídicos imateriais, de Joseph Kohler, que reconhece ao autor um direito absoluto *sui generis*, de natureza real. Paralelamente, declara existir uma relação jurídica de natureza pessoal entre o autor e a obra, que não constitui um elemento do direito autoral e conserva as características de puro direito da personalidade.

Como vemos, a propriedade intelectual já encontra no atual estágio da ciência do direito posições assentadas. Institutos como o *copyright* já contam com mais de 250 anos de existência no ordenamento positivo de algumas jurisdições.[23] Analogamente pode-se referir ao *Droit d'auteur* e a patente. Em construções mais modernas, pode-se citar ainda a nova proteção *sui generis* conferida pelo Tratado de Washington, assinado em 1989, aos circuitos integrados.[24]

Isto posto, deve-se acrescentar uma nova proposição. Durante muito tempo os bens jurídicos imateriais de uma forma geral foram confundidos com os objetos protegidos pelos institutos da propriedade intelectual. Não se deve pensar que só porque os bens como a invenção ou a criação, protegidos pela propriedade intelectual foram durante muito tempo os únicos bens imateriais mensuráveis, aferíveis e protegidos pelo direito patrimonial,

22. Newton Paulo Teixeira dos Santos, *A Fotografia e o Direito do Autor*, Leud, Rio, 1990, p. 17.

23. Um exemplo seria a lei sancionada pela Rainha Anne Stuart da Inglaterra, em 1710, estabelecendo privilégios com a duração de 21 anos para os autores de obras literárias e de 14 anos para os demais tipos de obras. Para um aprofundamento, veja a obra de L. Ray Patterson, em especial *Copyright in Historical Perspective* e, *The Nature of Copyright*.

24. Este Tratado assinado sob os auspícios da Organização Mundial da propriedade intelectual foi assinado em 26.5.89 e ainda não entrou em vigor.

que eles são os únicos bens imateriais relevantes para o Direito atualmente. Um instituto diferente da propriedade intelectual é o do segredo de indústria ou de comércio, também já respaldado por diversas legislações, onde o bem tutelado é essencialmente uma informação ou conhecimento, e não uma criação intelectual.

Fora da esfera patrimonial do direito privado, têm-se, no campo dos direitos fundamentais da pessoa humana, a tutela de bens imateriais, aí, de uma aferibilidade e mensurabilidade mais subjetiva, mas nem por isto inexistentes ou irrelevantes. Tais direitos também já são assegurados e protegidos por inúmeros dispositivos legais, tanto na comunidade internacional quanto nas diversas legislações.[25]

Para os crimes já previstos por estas três modalidades de *corpus legis*[26] contra estes diferentes objetos jurídicos, o computador vem trazer novos desafios e formas quanto ao meio de cometimento de tais delitos. A detecção e a efetiva acusação de crimes já tipificados nos quais utiliza-se o computador torna-se muito mais difícil. Como, também, pode se tornar maior o grau de reprovabilidade da conduta face ao maior dano causado por crimes contra tais bens empregando-se a informática. O computador então é usado para a prática de um delito, do mesmo modo que outros apetrechos. Discute-se, então, a criminalização de tais meios de cometimento, visto que certos crimes tornam-se impossíveis de tipificar, provar e processar quando praticados no ambiente informático.

As disposições de natureza penal para a proteção dos bens imateriais protegidos por estes institutos jurídicos, quando relacionados com a informática estão abrigados no estudo do que se convencionou chamar *Criminal Information Law* ou Direito Criminal de Informática, muito embora, na nossa opinião, não constituam crimes de informática, como veremos mais adiante.

3.6 Do bem ou Interesse a ser tutelado e protegido

Discute-se agora, a proteção a bens jurídicos redefinidos em sua importância, como o dado, a informação e as redes de computadores. Tal redefinição, é proveniente, como já nos referimos, anteriormente, das transformações sofridas pela sociedade pós-industrial, com o impacto causado pela moderna tecnologia da informação.

Primeiramente vamos definir estes termos. "Dado" pode ser entendido 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

25. O direito à privacidade vem, desde a Declaração Universal dos Direitos do Homem, sendo repetido por várias constituições e cartas internacionais. Porém, mais especificamente no âmbito da Informática, algumas destas leis de proteção à intimidade apareceram nos EEUU em 1974, na Alemanha e na Finlândia em 1977, e na Áustria, Dinamarca e França em 1978.

26. Constituição Federal de 1988 e Lei de Imprensa, Lei 5.250/67 alterada pela Lei 7.300/85, Código de Propriedade Industrial, Dec.-lei 7.903/45 e Lei do Direito do Autor, Lei 5.988/73.

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.

Para o computador todo o dado é uma informação, quer como registro, quer como instrução, respectivamente, fim e meio, mas para nós, só certos dados ou grupos de dados constituem informações que poderão ou não formar ou ser parte de um certo tipo de conhecimento. Tanto o dado quanto a informação não são adventos da *post industrial information society*. A informação sempre foi muito valorizada, constituindo verdadeira forma de poder, seu controle. *Information have always been power*. Isto é muito facilmente constatável, através dos tempos. Desde o Egito, por exemplo, os Faraós cercavam-se de sábios.

Os dados, quando referidos em relação aos sistemas de computadores ou de comunicação constituem objetos tangíveis, objetivos, porque estão, ainda que de uma forma muito tênue, individualizados, através de orifícios microscópicos e áreas lisas com propriedades reflexivas diferentes, no caso da tecnologia digital, comparáveis, por exemplo aos *corpus mechanicum* do Direito do Autor. Os dados então, servem como suportes dos objetos imateriais, subjetivos, que são as informações, por sua vez comparáveis aos *corpus mysticum*. Os dados também têm, através da história, sua importância registrada em exemplos como a destruição da Biblioteca de Alexandria por exércitos saracenos sob o comando do Califa de Omar em 638 dC.[27]

Daí, não concordarmos com Sieber que, ao fundamentar sua teoria, avalia e define a informação como um novo patrimônio econômico, político e cultural e, ainda, com um específico potencial de perigo. Concordamos, entretanto, com a afirmação que a moderna tecnologia da informação alterou as características da própria informação, especialmente por alargar sua importância e por tratá-la como um fator que trabalha sem a intervenção do homem, em processamento de dados automatizados.

Acreditamos que, quando uma mudança quantitativa alcança volume extraordinário, em algum ponto, ela se transforma em mudança qualitativa. A informática trouxe um novo desafio no lidar com informações e dados. É essa mudança que, agora, afeta o direito.[28]

A informação, quantificada e aferida através dos dados armazenados de forma objetiva em um sistema de informação, geralmente um sistema de computador, passará a ser a base da riqueza, do conhecimento e do poder da sociedade pós-industrial. Os dados e informações, uma vez que têm sua importância maximizada na sociedade informatizada pós-industrial, devem receber a proteção da tutela criminal, em todos os aspectos.

27. Alexandria Library, an Egyptian library loundad 290 BC by Ptolemy Soter of Alexandria and enriched by successive rulers. Destroyed by Saracen armies under Caliph Omar in 638 AD, it is thought the collection reaached 700.000 volumes.

28. Peter B. Maggs, John T. Soma, James A. Sprowl, op. cit., p. 504.

Porém, é necessário atentar para esta diferença entre dado e informação. No âmbito dos Crimes de Informática puros, inclusive como proposto no projeto, o termo "dado" deve ser utilizado, por ser mais objetivo, que "informação". Isso, porque informação é, como já exposto, um conceito muito vago para ser utilizado na lei penal. *A vox* só deve ser empregada no âmbito da proteção à privacidade. Esse também é o entendimento de Kaspersen,[29] constante da Exposição de Motivos do Ministro da Justiça Holandês, quando firma: "The term information applies to the result of a process rather than to the object of any (illegal) act. Under the present substantive criminal law, information or equivalent terms occur only in provision in which the process of obtainning informatin (illegally) is at stake, e.g. espionage, professional secrecy, trade secrets, insider trading. Therefore, the term computer data will be introduced in the Criminal Code, which not only refers to the content and meaing but also to the form and techinical environment of the potential information."

3.7 Das Redes de Computadores

As redes de computadores, desde os serviços mais simples até os mais complexos EDI, ou transferência de crédito eletrônico, caracterizam-se por serem sistemas de computadores interligados por equipamentos de telecomunicação.[30] Tais redes constituem-se em verdadeiros meios e modo autônomo de produção de riqueza e de prestação de serviços, sendo a base de muitas estruturas essenciais e complexas em nossa sociedade. Como Wasik[31] relata, os computadores são agora o centro de todo o mercado financeiro, bem como de muitos outros setores da economia. A informatização da Bolsa de Valores da City de Londres, por força de lei, não necessitará de mais nenhuma prova física das transações efetuadas. Com isto, se os computadores da City de Londres falharem, todo o complexo financeiro pára. Essas redes, embora não constituam em si mesmas, um bem jurídico, podem ser descritas como o recurso disponível de forma confiável, proveniente da utilização de sistemas de computadores, programas, bases de dados, e sistemas de comunicação.

Este não é um novo bem jurídico, mas é um novo meio advindo diretamente da moderna tecnologia. A rede pode representar o conjunto de recursos proporcionados pelo ambiente resultante da junção de diferentes sistemas de computadores interligados. Hoje em dia, as redes tornaram-se tão importantes que merecem ser protegidas e mantidas livres de qualquer interferência e mal uso. Isso porque, além de serem depositárias de confiança de vários segmentos da economia, como meio e modo de produção, requerem uma quantidade de recursos financeiros muito grande para serem mantidas.

29. Henrik Kaspersen, "Computer Crimes and Other Crimes against information Technology in the Netherlands — National Report", *International Review of Penal Law*, "Computer Crime and Other Crimes Against Information Technology" Erès, France, 1993, p. 470.

30. Alguns exemplos destas redes são: Access, Westlaw, Nexis, Lexis, EFT, Switf, Bitnet, Arpanet, UUCP, Internet, Dec Enet, Videotext, Genie, Compuserve, Reuters, etc.

31. Wasik, op. cit.

Além disto, abrigam uma capacidade de processamento e uma gama de informações e dados que não devem sofrer uso ou interferência não autorizada por quem quer que seja. O uso da rede e o uso de computadores isolados variam. Para utilizar um exemplo de fácil assimilação no mundo acadêmico, basta imaginarmos ao que seriam reduzidos os recursos de WWW, WAIS e Gopher, encontrados no Internet, se não fossem as redes de computadores.

Entendemos que crimes de informática ou crimes de computador são somente os atentados contra os dados e/ou informações, levando-se ainda em conta, a importância das redes, criminalizando-se então o meio de atacar os dados, informações e os próprios sistemas. Fica, desde já ressalvado, que esses crimes, além de ofenderem ao bem jurídico protegido, devem também preencher requisitos específicos para configurarem crimes de informática. Sem esses requisitos específicos, as ofensas continuarão acontecendo, contudo, sem serem caracterizadas, pelo menos do ponto de vista do projeto brasileiro, como verdadeiros crimes de informática. Tais requisitos serão examinados a seguir.

3.8 Definição de Crime de Informática

Em Direito, as palavras devem ter significado específico. O conjunto dos *nomina iuris* forma a chamada terminologia jurídica. Se temos que saber a definição de todos os termos jurídicos para podermos estudar o Direito, é necessário delimitar a extensão deles. Essa é a forma adequada ao estudo de qualquer ciência, pois condição primária para o progresso de qualquer delas é a pureza de seus conceitos e a propriedade de seus termos. A ausência de unanimidade na doutrina sobre a definição ou mesmo a natureza do crime de informática traz inúmeras dificuldades.

Wasik sustenta que o crime de informática é um tópico difícil e onde não é fácil haver o consenso sobre sua definição, não constituindo uma categoria legal precisa.[32] Assim, por exemplo, Parker e Nycum definem o crime de informática como qualquer ato ilegal onde um conhecimento especial de tecnologia de informática é essencial para a sua execução, investigação e acusação.[33] A polêmica é grande e a terminologia não é pacífica. Para demonstrar isso, basta dizer, que um mesmo autor ora emprega a expressão "crime do computador", ora "crimes cometidos através do computador".[34] Encontramos ainda: "Criminalidade mediante Computadores", "Criminalidade do Computador", "Delito Informático", "Criminalidade da Informática". Cada uma dessas denominações, porém, expressa, apenas, alguns aspectos de tais delitos e, como esclarece René Dotti, o interesse de precisar a denominação de uma disciplina específica leva em consideração não somente as características da realização do fato punível, como, também,

32. Martin Wasik, "Crime and the Computer", *Oxford Monographs on Criminal Law and Justice*, Oxford University Press, Oxford, 1991, p. 1.

33. D. B. Parker, S. Nycum and S. Aura: *Computer Abuse*, Menio Park, Calif.: Stanford Research Institute, 1973.

34. Valdir Sznick, "Crimes Cometidos Através do Computador", in *Novos Crimes e Novas Penas no Direito Penal*, Edição Universitária de Direito, S. Paulo, 1992, pp. 3 a 30.

as peculiaridades da conduta e os traços do caráter e da personalidade do seu autor.[35]

No Brasil, houve um tempo em que preferimos usar a expressão da língua inglesa — *computer crime* — por falta de uma palavra que, em nosso idioma, expressasse o conteúdo total de tais delitos.[36] Hoje, a terminologia de "Crimes de Informática", nos parece ser a expressão que mantém o sentido mais fiel e que melhor exprime o conteúdo de tais condutas em nossa língua.

Fundamentalmente, o "crime de informática" caracteriza-se por ser uma conduta lesiva, a qual não necessita, corresponder a obtenção de uma vantagem ilícita. Nesse conceito, não se incluem aquelas condutas que caracterizam crimes tradicionais, que têm por objeto material os sistemas de computação, seus componentes ou periféricos, como, por exemplo, o furto de material como *hardware* ou *software*. Assim, quem subtrai um computador pessoal com ânimo de vendê-lo e, com isso, obter dinheiro para seus gastos, estará cometendo um furto comum e não um "crime de informática".[37-38]

Definiremos então crime de informática, primeiramente, através do bem jurídico protegido. 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. Tal atentado deve dar-se contra os dados que, por sua vez, trabalharão sem a intervenção do homem, sendo estes o objeto material do crime.

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.

Deve-se, então, dizer que estes dois elementos são indissociáveis, pois, prevalecendo apenas um deles, não se estará diante de um crime de informática, mas sim de um crime comum, ou já tipificado, perpetrado através do uso do computador. Assim, o agente que explode um edifício para tornar irrecuperáveis arquivos contidos em fitas magnéticas que estavam ali estocadas, atenta contra um bem, bem precioso, que são, em primeira análise os dados contidos nestas fitas e que podem ser traduzidos em informações. Mas, nem por isto estará cometendo um crime de informática. Isto, por falta do segundo elemento. Assim, aquele que usa um computador para matar um doente gravemente enfermo, ligado à aparelhos de manutenção de vida em um C.T.I., estará cometendo homicídio, e não crime de informática, pela falta do primeiro elemento.

35. René Ariel Dotti, *Reforma Penal Brasileira*, Forense, Rio, 1988, p. 359.

36. João Marcello Araujo Junior, "Computer Crime", in *Anais da Conferência Internacional de Direito Penal*, outubro de 1988, Procuradoria Geral da Defensoria Pública, Rio, 1991, p. 459.

37. Este é, também, o pensamento de Michele M. Correra e Pierpaolo Martucci: *I Reali Commessi con l'uso del Computer*, CEDAM, Padova, 1986, p. 26.

38. Um estudo da American Bar Association demonstrou que mais de um bilhão de dólares são perdidos anualmente com este tipo de furto nos EEUU.

Queremos então dizer, que nem todo atentado contra os dados, as informações e as redes de computadores constituirão crimes de informática. Poderão constituir qualquer dos crimes já tipificados, ou ainda ilícitos civis ou administrativos, já que um mesmo bem jurídico pode ser atacado, e conseqüentemente protegido em vários campos do Direito.

3.9 Do sujeito ativo dos crimes de informática

Até um passado recente, em países desenvolvidos, especialmente nos EEUU, os criminosos, após serem condenados a penas leves eram contratados como especialistas em segurança e consultores de informática.

Porém, a história mostra que os crimes de informática são cometidos pelos mais variados tipos de pessoas, como por exemplo: estudantes, aficcionados, terroristas, membros do crime organizado e profissionais.

Não entendemos os crimes de informática como somente perpetráveis por um indivíduo altamente especializado e talentoso, geralmente chamado de *expert*. Daí não podermos concordar com Parker[39] que, em seu trabalho pioneiro, assim descrevia os agentes: "Perpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technicall challenge. They have exactly the characteristics that make them highly desireble employees in data processing".

Isso mostra, como a sociedade tecnológica evolui rapidamente. Tal definição, dada no início dos anos 70, revela como o mito suplantava a realidade. Hoje, não podemos concordar com tal definição, inclusive por coerência, uma vez que não vemos, por exemplo, em cada homicida à mão armada, um especialista em balística e em armamento, pronto para ser incorporado aos órgãos responsáveis pela segurança da população ou do Estado.

Hoje, já é sabido, que qualquer pessoa, de qualquer idade com um mínimo de habilidade, motivada pela mudanças e inovações tecnológicas ou, pela perspectiva de obtenção de notoriedade, recursos ou ainda movida pelo desejo de satisfazer sentimentos ou interesses é potencialmente agente dos crimes de informática. Some-se a estes argumentos o que sustenta a Associação dos Delegados de Polícia do Canadá, citada no Manual sobre Crimes de Informática da ONU.[40] "The typical skill level of the computer criminal is not an indicator of a computer criminal..."

4. Considerações sobre a criminalização de certas condutas

4.1 Da criminalização de novas condutas

A proposta da nova parte especial do Código Penal a ser apresentada pelo Poder Executivo ao Congresso Brasileiro, no que diz respeito a tutela penal dos interesses e dos bens advindos, ou redefinidos em sua importância,

39. Donn Parker, *Fighting Computer Crime*, New York, Charles Scribner's Sons, 1983. Veja também do mesmo autor *Crime By Computer*.

40. "The Canadian Association of Chiefs of policy, Computer Security Guidelines", (Ottawa, 1989), citado no *Manual das Nações Unidas sobre Crimes relacionados com computadores*, p. 9.

pela *post industrial information society*, caracteriza-se, por estabelecer um caminho próprio, fundado nos argumentos já examinados.

Os crimes de informática estão contidos em um Capítulo, do Título denominado "Dos Crimes Contra a Ordem Socioeconômica", da Parte Especial do Código Penal. O mencionado Capítulo conta com, apenas, oito artigos. Três destes artigos tratarão especificamente dos crimes de informática, como definidos anteriormente, enquanto outros três dispositivos tratarão da adequação de normas já existentes aos bens intangíveis redefinidos em sua importância, enquanto, outros dois têm a finalidade de reprimir atos de atentado considerados especialmente graves à privacidade dos indivíduos, e, perpetrados através do computador. Podemos dizer que, enquanto três artigos tratarão de *Computer Crime*, outros cinco estarão relacionados com os *Computer Misuse*.

4.2 Da lei penal substantiva

A legislação brasileira em matéria de crime de informática é muito pobre. As normas penais incriminadoras constantes de nosso direito positivo são de um tempo em que os delitos de que estamos tratando, não estavam na ordem do dia. Por isso, as normas contidas no Código Penal, cuja Parte Especial data de 1940, somente de forma incidental são aplicáveis a tais hipóteses.

A preocupação da legislação atual dirigiu-se especialmente para o crime de "pirataria de *software*", o que consideramos, como já mencionado um *Computer Misuse*, mas não um crime de informática.

A orientação da doutrina brasileira acompanhou a tendência internacional que protege do *software* à moda do direito autoral. Essa posição doutrinária foi aceita pelo legislador, que na Lei de Defesa do *Software*, Lei 7.646, de 18.12.87, definiu em seus arts. 35 e 37 dois crimes que expressam esse entendimento. No art. 35, pune com detenção de 6 (seis) meses a 2 (dois) anos e multa, a ação de "violar direitos de autor de programa de computador" e no art. 37, um tipo que poderíamos denominar criticamente de "contrabando de *software* não cadastrado", estando assim definido: "importar, expor, manter em depósito para fim de comercialização programas de computador de origem externa não cadastrados: pena: detenção de 1 (um) a 4 (quatro) anos e multa". Este último crime tem natureza econômica, uma vez que se destina a fortalecer, com a sanção penal, as regras de reserva de mercado estabelecidas por nossa política nacional de informática, como já mencionado.

Como é de fácil demonstração, pela simples leitura, as regras legais citadas são manifestamente imperfeitas e insuficientes para os fins a que se destinam, tanto assim, que, com a mudança de nossa política de reserva de mercado em matéria de informática, como veremos mais adiante, em breve o delito de "contrabando de *software* não cadastrados" será descriminalizado.

A lei brasileira protege a propriedade intelectual, em relação ao programa de computador, como manifestação da propriedade imaterial, fazendo-o da mesma forma que o Código Penal o faz, para a violação do direito autoral em geral. Entretanto, a pena prevista é mais severa que aquela cominada no Código Penal (detenção de três meses a um ano e multa). A

Lei que define crimes contra a ordem tributária, econômica e contra as relações de consumo, Lei 8.137, de 27.12.90 definiu uma nova forma de *Computer Misuse* vinculada à ordem tributária. Trata-se da ação de utilizar ou divulgar programa de processamento de dados que permita ao sujeito ativo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Pena: detenção de 6 (seis) meses a 2 (dois) anos, e multa." Trata-se, como se vê, de um programa de computador especificamente destinado a permitir a fraude fiscal, ou seja, uma hipótese em que a informática é utilizada pelo instrumento do crime, configurando um *Computer Misure*. Essa é toda a nossa legislação em matéria de Direito Penal de Informática. Diante dessa quase indigência normativa, vê-se o aplicador obrigado a servir-se dos delitos tradicionais para combate a essa nova forma de criminalidade. É possível o enquadramento de algumas condutas na figura tradicional do estelionato. Entretanto, questões ligadas à natureza da fraude e às relações entre os sujeitos da relação criminal, nem sempre permitem o estabelecimento da tipicidade. Bem sabemos, que no momento atual do desenvolvimento científico, as principais correntes do pensamento que se envolvem com o fenômeno da criminalização propugnam por um amplo programa de descriminalização. Os neodefensistas o fazem em função da perda do interesse social na punição de determinadas figuras legais de crime. Já os adeptos da Criminologia Crítica e os do seu consectário, a Política Criminal Alternativa, assim pensam também, porém, em contemplação de um direito penal mínimo, limitado pelos Direitos Humanos, como afirma Baratta.[41] Ocorre que, tanto para os neodefensistas como para os criminólogos críticos, a moderna política criminal se caracteriza por uma dupla via, ou seja, ao lado do movimento de descriminalização existe um outro, em sentido inverso, destinado a criminalizar fatos novos ligados às modernas formas de criminalidade.[42]

Diante desse quadro teórico-prático a tendência no Brasil é no sentido da criação de alguns tipos legais de crimes específicos. Tal tendência se manifesta pela análise dos projetos de lei em tramitação no Congresso Nacional. Atualmente, estão em tramitação no Congresso Nacional os seguintes Projetos:

A) Projeto de Lei do Senado n. 75 de 1989, que "Dispõe sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas". Tal projeto foi absorvido por outro, de n. 137 de 1989, que tem a seguinte redação:

"Art. 1.º. Constituem crimes contra a liberdade individual:

I — violar, mediante processo técnico ou qualquer outro meio, o resguardo sobre foto, imagem, escrito ou palavra da vida privada de alguém;

Pena — detenção de três meses a um ano.

41. Alessandro Baratta: "Principios del derecho penal mínimo", in *Anais da Conferência Internacional de Direito Penal*, Procuradoria Geral da Defensoria Pública, Rio, 1991, p. 21.

42. Evandro Lins e Silva: "De Beccaria e Felipo Gramatica", in João Marcello de Araujo Junior (organizador): *Ciência e Política Criminal em Honra de Heleno Fragoso*, Forense, Rio, 1992, p. 21.

II — fornecer ou utilizar, indevidamente, dado da vida privada de alguém, constante de fichário automatizado;

Pena — detenção de três meses a um ano.

Art. 2.º. As penas cominadas no artigo anterior serão aumentadas até o dobro, se o agente houver atuado com fim de lucro ou abuso de função.

Art. 3.º. A ação penal, nos crimes previstos nesta lei depende de representação."

B) Projeto de lei da Câmara dos Deputados n. 4.597, de 1990, substituído pelo de n. 597, de 1991, que "Dispõe sobre o crime de interferência nos sistemas de Informática", possuindo a seguinte redação:

"Art. 1.º. Pratica de crime quem, objetivando proveito ilícito, para si ou para outrem, ou ainda visando a causar prejuízo a alguém, a um sistema, a computador, a equipamento que componha o sistema ou a programa:

a) destrua ou altere, dolosamente, ou utilize de modo indevido, programa de computador a que tem acesso;

Pena: detenção de um a cinco anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

b) abuse, por qualquer outra forma, de seu direito de acesso a computador, a sistema de computação, de transmissão de dados, ou de processamento de dados de qualquer espécie;

Pena: detenção de um a quatro anos e multa igual ao valor do proveito visado ou do risco do prejuízo da vítima;

c) introduza, dolosamente, em computador, programa ou instrução-comando que destrua ou altere programa armazenado no computador, ou por qualquer forma altere o seu desempenho;

Pena: detenção de um a quatro anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

d) utilize senha de outrem para obter acesso indevido a um sistema ou a um computador;

Pena: detenção de um a três anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

e) obtenha intencionalmente, sem estar devidamente autorizado, acesso a um sistema ou a um computador;

Pena: detenção de um a três anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

Art. 2.º. A interferência não intencional, por negligência, imprudência ou imperícia, constitui crime culposo.

Pena: multa igual ao prejuízo causado. Mínimo de Cr$ 170.000,00 (cento e setenta mil cruzeiros). Na reincidência, detenção de um a três meses e multa igual."

No que diz respeito à proteção aos programas de computador, o Exmo. Sr. Presidente da República dando seqüência à política de liberação em matéria de Informática, enviou ao Congresso Nacional a Mensagem n. 229/91, que assumiu a denominação Projeto de Lei 997/91, que "dispõe sobre a proteção da propriedade intelectual de programas de computador, sua comercialização no País e dá outras providências". Como está dito na Exposição de Motivos que acompanhou a Mensagem Presidencial, o Projeto segue, fundamentalmente, as seguintes diretrizes: a) eliminação das restrições

a empresas nacionais para distribuição e comercialização de programas de computador de origem externa no País; b) eliminação do exame de similaridade entre o produto estrangeiro e o nacional; c) eliminação do cadastramento de programas de computador; d) possibilidade de importação de cópias de programas de computador sem contrato de distribuição, objetivando maior competitividade do setor; e) reforço aos direitos e garantias dos usuários de programas de computador.

O crime de violação do direito autoral de programa de computador (art. 35 da Lei atual), no Projeto, não sofre alteração, seja quanto à sua definição típica, seja quanto a quantidade e qualidade da pena.

As maiores e mais importantes inovações estão previstas no Projeto de Lei do Senado n. 152, de 1991, de autoria do Sen. Maurício Corrêa e, principalmente, do substitutivo apresentado ao Projeto. No aludido Projeto, sente-se que a maior preocupação do legislador é garantir os dados de propriedade do usuário. Assim, o bem jurídico a ser protegido é a invoabilidade dos dados e da sua comunicação. Além disso, ao autor do Projeto pareceu que, salvo importantes exceções, o emprego da informática não teria criado novas figuras criminosas, mas, apenas, se transformado em novo meio para o cometimento de crimes tradicionais, razão pela qual a lei deveria, além de criar umas poucas figuras criminais, ocupar-se em criar mecanismos legais que permitam a aplicação das normas contidas no Código Penal a tais ilícitos.

Dentre os novos delitos previstos no Projeto, destaca-se o de acesso indevido à informação de outrem. Tal delito destina-se a dar execução ao comando constitucional que garante o sigilo de dados.

Quanto aos chamados "vírus", a responsabilidade penal não deve se limitar, apenas, ao criador do programa, devendo alcançar principalmente aquele que o insere em sistema alheio. Daí, a conduta punível dever caracterizar-se pela ação de "colocar em circulação" um programa "vírus". Ademais disso, para ser criminoso, o "programa vírus" não precisa trazer vantagem para o sujeito ativo das relações criminais, nem prejuízo econômico para o sujeito passivo, bastando a provocação de algum efeito indesejado no sistema atingido. Daí ser o seguinte, o texto do substitutivo ao Projeto 152/91:

"Art. 1.º. Consideram-se crimes contra a inviolabilidade dos dados a sua comunicação a prática das condutas descritas nos arts. 2.º e 3.º desta lei.

Art. 2.º. Violar o sigilo de dados, acessando informação contida em sistema ou suporte físico de terceiro, sem autorização deste.

Pena: Detenção de um a seis meses ou multa.

§ 1.º. Se o acesso de faz com uso indevido de senha ou de processo de identificação magnética de terceiro.

Pena: Detenção de três meses a um ano e multa.

§ 2.º. Se do acesso resultar vantagem econômica indevida, em detrimento do titular do sistema, pune-se o fato como estelionato qualificado nos termos do art. 4.º desta lei.

Art. 3.º Inserir em suporte físico de dados, ou em comunicação de dados, programa destinado a funcionar clandestinamente no sistema de terceiro, causando nele efeito indesejado por seu titular.

Pena: Detenção de um a seis meses e multa.

§ 1.º. Se resulta perda definitiva de informação contida no sistema.

Pena: Detenção de seis meses a dois anos e multa.

§ 2.º. Se, além da perda de informação, resulta prejuízo econômico para o titular do sistema.

Pena: Detenção de um a três anos e multa.

Art. 4.º A realização de conduta descrita nesta lei como meio para a prática de qualquer outro crime qualifica-o, agravando a pena de um sexto até a metade.

Art. 5.º. A informação ou dado constante de sistema eletrônico que, por qualquer razão, tenha relevância nas relações entre pessoas, considera-se "documento", punindo-se sua adulteração material ou ideológica nos termos do Código Penal, com a qualificadora do art. 4.º desta lei.

Parágrafo único — Para os fins deste artigo considera-se "documento público" a informação ou dado constante de sistema:

a) pertencente ou a serviço de órgão público da administração direta ou indireta, instituição financeira, Bolsa de Valores ou estabelecimento de ensino oficial ou reconhecido;

b) em condições de autorizar pagamento, quitação movimentação de conta corrente ou qualquer transferência de valores;

c) destinado ao acesso público, pago ou gratuito, a informações comerciais, econômicas ou financeiras."

Esta era a tendência do direito brasileiro no momento atual, sendo certo que a criminalização dos crimes de informática ocorreria em lei extravagante (que vaga fora do Código Penal).

Agora, esperamos que a contribuição dada ao projeto da nova parte especial do Código Penal represente uma evolução ao atual estágio do Direito Penal de Informática em nosso país.

4.3 Proposta para a nova Parte Especial do Código Penal

Dos Crimes contra os Sistemas de Processamento ou Comunicação de Dados:

VIOLAÇÃO DE SISTEMA DE PROCESSAMENTO OU COMUNICAÇÃO DE DADOS

Art. 1.º. Violar, obtendo ou tentando obter acesso, indevidamente, sistema de processamento ou de comunicação de dados alheio, fazendo-o produzir qualquer função:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos.

Formas Qualificadas:

§ 1.º. Se o acesso indevido tem por fim causar dano a outrem ou obter qualquer vantagem:

Pena: ... multa e interdição para o exercício da atividade ligada à informática por ... anos

§ 2.º. Se com o acesso indevido o agente produz alteração temporária ou permanente, em dado, instrução ou programa de computador constante ou acessável por sistema de processamento ou comunicação de dados:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

§ 3.º Se o acesso indevido ou a alteração de dado, instrução ou programa de computador se fizer com o uso de senha ou outro processo de identificação de outrem:

Pena: ... multa interdição para o exercício de atividade ligada à informática por ... anos.

§ 4.º. Se com o acesso indevido o agente devassa o sigilo de dado constante, ou acessável por sistema de processamento ou de comunicação de dados:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

§ 5.º. Se com o acesso indevido ou com a alteração de dado, instrução ou programa de computador o agente causa dano a outrem ou obtém qualquer vantagem:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

ATENTADO CONTRA A INTEGRIDADE DE SISTEMA DE PROCESSAMENTO OU COMUNICAÇÃO DE DADOS

Art. 2.º. Desenvolver comando, instrução ou programa de computador capaz de, clandestinamente, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa de computador ou, provocar qualquer outro resultado diverso do esperado em sistema de processamento ou comunicação de dados, com o fim de causar dano a outrem, obter indevida vantagem ou satisfazer sentimento ou interesse pessoal:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

CONTAMINAÇÃO DO SISTEMA DE PROCESSAMENTO OU COMUNICAÇÃO DE DADOS

Parágrafo único. Nas mesmas penas incorre quem introduz o comando, instrução ou programa de computador a que se refere este artigo, em sistema de processamento ou comunicação de dados alheio.

SABOTAGEM INFORMÁTICA

Art. 3.º. Destruir, inutilizar ou deteriorar o funcionamento ou a capacidade de funcionamento de sistema de processamento ou comunicação de dados alheio, com o fim de causar dano a outrem, obter vantagem ou satisfazer interesse ou sentimento pessoal.

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

Parágrafo único. Nas mesmas penas incorre quem, com o mesmo fim:

I — apaga, elimina, altera, grava ou transmite dado, instrução ou programa de computador constante de suporte físico, sistema de processamento ou comunicação de dados alheio;

II — provoca qualquer outro resultado diverso do esperado, que viole a integridade ou a confiabilidade de dado, instrução ou programa de computador constante de suporte físico, sistema de processamento ou comunicação de dados alheio.

FURTO DE TEMPO DE REDE DE SISTEMA DE PROCESSAMENTO DE DADOS

Art. 4.º. Utilizar, sem autorização de quem de direito, recurso de rede de entidade governamental ou de caráter público de sistema de processamento ou comunicação de dados:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

TRÁFICO DE DADOS PESSOAIS

Art. 5.º. Destinar dado ou informação de caráter pessoal, constante de sistema de processamento de dados ou de qualquer suporte físico, a pessoa não autorizada ou a fim diverso daquele ao qual a informação se destina, sem permissão do interessado:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

Parágrafo único. Nas mesmas penas incorre quem, nas condições deste artigo, obter o dado ou a informação de caráter pessoal.

VIOLAÇÃO DO DEVER DE INFORMAR

Art. 6.º. Deixar de dar conhecimento ou retificar informação pessoal constante ou acessável por sistema de processamento ou comunicação de dados ou de suporte físico de entidade governamental ou de caráter público, quando exigido pelo interessado:

Pena: ... multa e interdição para o exercício de atividade ligada à informática por ... anos

EQUIPARAÇÃO A DOCUMENTO

Art. 7.º. Considera-se documento, para efeitos penais, o dado ou programa de computador constante de sistema de processamento ou comunicação de dados ou de qualquer suporte físico.

CRIMES DEFINIDOS EM OUTROS CAPÍTULOS

Art. 8.º. O Crime não definido neste Capítulo, quando cometido com o emprego de sistema de processamento ou comunicação de dados, terá sua pena aumentada de ...