Crimes de informática

Introdução e História do Computador

Marco Aurélio Rodrigues da Costa*

INTRODUÇÃO

Não existe nenhum nicho tecnológico que se desenvolveu tanto e com tanta velocidade como o dos computadores.

O I Plano Nacional de Informática e Automação, chegou a ser considerado como o verdadeiro passaporte estratégico para colocar o Brasil no mundo da informática e ser mola propulsora do nosso próprio desenvolvimento.

Abstraindo-se tal ilação, devemos nos render a realidade: estamos nos informatizando em velocidade acima do que até se pode notar, ou seja, muito rapidamente. Tal constatação vem pelos dados que nos são alcançados pelos serviços especializados, porém, e nem seria necessário, pois basta que voltemos nossos olhos para as bancas de revistas para ver uma gama de publicações especializadas na área de informática, ou abrir os cadernos de anúncios classificados de nossos jornais que veremos o crescimento abrupto de ofertas de equipamentos, cursos, sistemas, periféricos, etc, ou, ainda, se isso não bastasse, numa rápida pesquisa em nosso meio social, veremos que há um número elevado de proprietários de computadores, número esse muito acima do que possamos imaginar.

A grande questão sobre essa verdadeira invasão dos computadores na vida das pessoas e das empresas, é saber os reflexos dessa tecnologia no mundo jurídico. São, por muito claro, tais reflexos indeléveis, vez que a sociedade se transforma com o uso e a dependência dos computadores, de modo que o Direito jamais poderá ser o mesmo.

Muito se tem falado de que os computadores são um instrumento que estão mudando, auxiliando o trabalho dos operadores do Direito, à medida em que racionalizam, organizam e aumentam a qualidade das tarefas do profissional do Direito. Todavia exsurge desse nicho tecnológico dois novos segmentos do Direito: o *Direito Civil da Informática e o Direito Penal da Informática*.

O que chamamos de Direito Civil da Informática, estrito senso, seria o conjunto de normas que regulariam as relações privadas que envolvem a aplicação da informática, quais sejam, computadores, sistemas, programas, cursos, direitos autorais, etc. O que denominamos de Direito Penal da Informática seria o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos que atentem contra o uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos, os computadores.

Para se ter uma idéia do quanto é importante que exista a regulação penal da informática, na Suíça as seguradoras perdem anualmente cerca de 6 milhões de francos, somente através de *crimes de informática*. Em 1984, na França, 700 milhões de francos foram perdidos em delitos de informática, valor este superior aos prejuízos com assaltos bancários no mesmo ano.

Muitos hão de pensar que tais perdas apenas apuram-se em países desenvolvidos. Ledo engano. Os mesmos delitos são perpetrados no Brasil, só que não são noticiados, e, na sua maciça maioria, não estão cobertos por seguro, como a exemplo do que ocorre nos Estados Unidos, que pelas suas características, as grandes empresas, não divulgam delitos que atingem os sistemas de computadores, pois se divulgados, seguramente, abalariam a credibilidade das empresas-vítimas.

Por outra, já é uma instituição mundial a inoculação, em todos os tipos de computadores, por vírus, principalmente os sistemas bancários, que geram incalculáveis prejuízos e, no Brasil, mais especificamente, estes destruidores de dados, arquivos e informações, vicejam impunes, por falta de legislação própria.

A revista *Exame Informática* (14, jun,1993, p.56) afirma que, na maioria dos casos conhecidos no País, os micros foram vítimas de vírus malignos. E, ainda, são citados pela revista o caso de vários PCs. da Universidade de São Paulo, PUC-RJ, Petrobrás, Banco Real, Indústrias Levonin, Amercian Express, White Martins, Embratel, BNDES, etc.

Reiterando, parece que no Brasil não são publicados os casos, porque o conhecimento da vulnerabilidade do sistema pode ser mais nefasto do que o próprio crime. De qualquer modo, o que vazou, já demonstra que os delitos de informática já estão, definitivamente, instalados em nosso País.

Para buscar uma fórmula jurídico-penal, Estados Unidos, Itália, Canadá, França, Espanha, Dinamarca, Alemanha, entre outros, estudam, através de comissões mistas de técnicos na área de informática e juristas, a implantação de legislação para coibir tais delitos, que se utilizam de extremo conhecimento técnico para praticarem atos que lesam o patrimônio de pessoas físicas e jurídicas, até pelo simples prazer de causar prejuízos, sem, inclusive, se locupletarem de tais condutas lesivas, na maioria das vezes, como é caso de inoculação de vírus.

No Brasil existem algumas tímidas iniciativas através de projetos de lei que ora tramitam no Senado e na Câmara Federal. Todavia, não atendem os anseios dos usuários de computadores, que esperam uma legislação forte e efetiva à prevenção, repressão e punição dos atos lesivos praticados por delinqüentes de informática.

Em razão disso é que nos arvoramos a escrever sobre *crimes de informática*, pretendendo levantar a origem do computador, elemento central da informática, buscando visualizar os caminhos que foram tomados pelos precursores da informática, da era denominada *"pós-industrial"*.

Temos, também, a pretensão de mostrar o quão deficiente é o Direito Penal brasileiro, quando se defronta com os delitos desta natureza, até porque a Parte Especial do nosso Códex material Penal data de 1940, e no Brasil o computador aportou em meados de 1960. Portanto, quase impossível de se aplicar a Parte Especial do Código Penal aos *crimes de informática*, porém, com vistas nos princípios gerais do direito penal, ainda, é possível serem aplicadas as regras da Parte geral da nossa Lei Penal aos delitos de informática".

Um dos temas mais difíceis entre os doutrinadores do Direito Penal de Informática é a conceituação e denominação. O conceito vem, em muitas oportunidades, de forma restritiva ou por demais abrangente. Não reflete as muitas situações em que se enquadram os *crimes de informática*. A denominação é, também, motivo de grande polêmica entre os estudiosos do Direito Penal de Informática, pois a cada denominação segue-se um conceito e, vice e versa. É, pois importante que se busque dissecar tais polêmicas.

O Direito Penal brasileiro tem em seu texto a fundamentação para ser implantado o Direito Penal de Informática, dele devem afluir as normas penais de informática.

Temos observado que os delinqüentes de informática nem sempre vislumbram o locupletamento material com a sua conduta antijurídica, objetivam o desafio ao equipamento, as regras de ética, pelo simples fato de satisfazerem-se intimamente ou contar apenas a vantagem que venceu barreiras de segurança. Por isso, é importante que se garimpe o elemento volitivo do agente ativo dos *crimes de informática*. Só assim se pode combatê-los com normas adequadas de modo a instrumentalizar-se o Estado na sua missão coercitiva.

De outra banda, o grande holocausto dos doutrinadores é o momento em que aportam na dicotomização do delito comum e o de informática. Muitos têm escrito inclinados a garantirem que não existem delitos desta ordem; outros entendem que, em razão da sua complexidade, deve ser revisto o próprio conceito de crime. O certo é que existem crimes comuns, crimes comuns de informática e *"crimes de informática"*.

Vemos que muitas condutas delitivas de natureza informática são difíceis de ser tipificadas, e até de serem criminalizadas, seja ao prisma das normas existes ou vislumbrando-se um novo direito. Assim, muitas propostas de criminalização são

lançadas aos *"crimes de informática"*, contudo, em sua grande maioria são deficientes ou carecedoras de conhecimento da própria informática, ou ainda, são propostas de normas que se sobrepõem às existentes.

Os *"crimes de Informática"*, devem, ao nosso entender, ser classificados adequadamente para que o legislador pátrio possa elaborar normas eficientes, e, se necessário, indicar as normas vigentes que podem ser aplicadas, porém é imprescindível estudo crítico dos delitos de informática.

Além da classificação é necessário que se busque individualizar as espécies de delitos de informática, assim instrumentalizaria o aprofundamento do objeto jurídico a ser protegido, bem como a aplicação da norma adequada, e a pena adequada ao delito.

Não pretendemos esgotar o tema, sabemos das limitações da obra, porém acreditamos que a discussão permanente sobre a matéria tem o condão de manter o alerta a esse novo direito que já não bate a nossas portas, mas já está entre nós, e, também, ampliar o que se apresenta "in vitro" sobre o Direito Penal de Informática.

HISTÓRICO DO COMPUTADOR

Qualquer obra que aborde o computador e suas características tem obrigatoriamente que trazer a sua história. Esta, recente, hipermoderna, determina que devemos saber que *computador=calculador; computação=avaliação, contagem; computar=avaliar, contar, calcular*.

Desde a época primitiva, o homem tenta de algum modo comunicar-se ou transmitir informações de sua existência para gerações futuras, através de hieróglifos gravados em tábuas de pedras e mapas de batalhas.

Para tanto, o homem conhece o valor de ferramentas auxiliares para facilitar seu trabalho físico e mental. Como exemplo, temos a carroça, que se tornou um meio de vencer as longas distâncias; o telescópio que é um prolongamento da visão; o telefone que é a extensão da nossa voz, e tantos outros.

Conforme a civilização evolui, o homem continua a procurar novos meios para facilitar sua vida e, dessa maneira, dominar as forças da natureza.

Trocando o animal pelo motor, chegou ao automóvel, ao transporte aéreo e a outros avanços muito mais sofisticados.

Após muitas pesquisas chegou ao computador eletrônico, um prolongamento do seu cérebro.

Pedrinhas (pastores gregos e egípcios)

Com as crescentes necessidades humanas, o homem sentiu a necessidade de proteger seus rebanhos. Para isso cercou-os. Mais tarde, necessitou ter um controle sobre eles, e é aí que surge o controle das pedrinhas, onde cada animal era representado por uma pedrinha, que acumuladas representavam o montante . O homem estava fazendo seu primitivo processamento de dados.

Ábaco

Um dos primeiros instrumentos no auxílio ao cálculo, podemos citar o Abaco, utilizado pelos primitivos mercadores egípcios e romanos, há cerca de 2.000 anos, para fazerem o cômputo de suas transações. No Abaco, os números eram representados por pedrinhas de calcário denominadas "calculi", de onde surgiu a palavra cálculo.

Os ossos de Napier

No início do século XVII, o escocês JOHN NAPIER, inventou um dispositivo que trouxe grande auxílio ao uso de logaritmos, em execução de operações aritméticas, como multiplicações e divisões longas. Este dispositivo tornou-se conhecido como "OSSOS DE NAPIER". Hoje, o dispositivo aperfeiçoado é empregado tão freqüentemente pelos engenheiros, através da régua de cálculo.

Primeiras máquinas de calcular

O precursor das máquinas de calcular, o matemático e filósofo francês, BLAISE PASCAL, construiu em 1642 uma máquina para somar e subtrair números de oito algarismos, baseada em engrenagens.

Em 1677, o também matemático e filósofo, o alemão GOTTFRIED LEIBNIZ, construiu uma máquina de calcular. Em meados de 1830 começa na Europa a fabricação em série de máquinas de calcular mecânicas.

Cartão perfurado

Em 1801, o tecelão francês, JOSEPH-MARIE JACQUARD, construiu uma máquina de tear comandada por cartões perfurados enfileirados.

Charles Babbage

Em 1834, BABBAGE construiu um modelo de máquina capaz de executar uma seqüência pré-determinada de operações onde foi embasada, genericamente, a organização de um moderno processador. A memória do processador aritmético e a entrada/saída são identificáveis nas descrições que deixou, assim como a idéia de armazenar dados em forma de comandos, e seqüências de operações a serem executadas sobre os comandos.

Entretanto, a tecnologia da época não estava à altura da tarefa de traduzi-la mecanicamente no equipamento. Mas, 100 anos após, seu trabalho foi estudado antes que o projeto HARVARD MACHINES (MARK I) fosse iniciado.

As máquinas de cartão perfurado

HERMAN HOLLERITH, funcionário do Departamento de Estatística dos Estados Unidos, em 1880, no recenseamento acusou uma população de 55 milhões de habitantes aproximadamente, sendo que a apuração demorou 7 anos, com 500 empregados. Preocupado com censo seguinte procurou meios para mecanizar o trabalho de apuração utilizando a idéia do tecelão francês JACQUARD.

Em 1885 iniciou-se a construção da máquina de cartão perfurado, e utilizada no censo de 1890, no qual a apuração levou cerca de um ano, com apenas 43 funcionários. Essas máquinas começaram a ser utilizadas com maior freqüência nas

mais diversas aplicações, nas repartições públicas, comércio, indústria, etc.

No princípio do século XX, essas máquinas foram aperfeiçoadas, realizando operações aritméticas elementares. Eram máquinas eletromecânicas muito lentas.

Calculadoras de relés

A partir de 1930, foram feitos vários estudos para construir calculadoras mais rápidas e versáteis com funcionamento baseado em relés eletromagnéticos. Em 1835, KONRAD ZUZE começa a desenvolver calculadoras de relés na Alemanha. Foram construídos os modelos Z1, Z2, Z3 e Z4. O modelo foi construído em 1914, sendo a primeira calculadora automática a trabalhar sob o controle de um programa perfurado em uma fita de papel.

Em 1937, nos Estados Unidos, HOWARD AIKEN, desenvolveu uma calculadora de relés na Universidade de Harvard. A primeira calculadora automática, controlada por programa, construída por AIKEN, ficou pronta em 1944 e recebeu o nome de MARK I.

ENIAC - o primeiro computador eletrônico

De 1934 a 1946, JOHN P. ECKERT e JOHN W. MAUCHLY, na Universidade da Pensylvania, construíram um computador baseado em circuitos eletrônicos, que recebeu o nome de ENIAC (Eletric Numeric Integrator and Calculator). Tinha 18.000 válvulas eletrônicas e utilizava o sistema de numeração binária, realizando uma operação de multiplicação de dois fatores de 10 algarismos em 0,003 segundos.

J0HN VON NEUMANN, construiu, em seguida, o computador eletrônico EDVAC, que utilizava a idéia de programação interna. Esta idéia consistia em armazenar dados do programa em forma de codificação, dentro da memória do computador, e

não num veículo externo, como a fita perfurada. Através de uma programação interna o computador pode executar instruções em qualquer ordem, e repeti-las, se necessário.

Generalização do uso do computador

O ENIAC e o EDVAC, foram modelos experimentais, e não foram explorados comercialmente. A partir de 1950, várias empresas começaram a fabricar computadores em série. Em 1951 foi anunciado o UNIVAC I, que iniciou a primeira geração de computadores. A INTERNACIONAL BUSINESS MACHINES (IBM) lança seu primeiro computador eletrônico, o IBM 701.

EM 1958, a SIEMENS, na Alemanha, lança o SIEMENS 2002. O IBM 1401 é o representante mais típico dessa geração. Dois anos mais tarde nos Estados Unidos, foi criada uma linguagem universal de programação para fins comerciais, por um grupo de representantes do governo, de fabricantes e usuários de computadores, a qual recebeu o nome de COBOL (Common Business Oriented Language).

Em meados da década de 1960, inicia-se a terceira geração de computadores, caracterizada pelo uso de circuitos monolíticos integrados e por avançados sistemas operacionais.

A década de 1970 sofreu grande revolução com o surgimento dos MICROPROCESSADORES. O surgimento dos micros deveu-se, basicamente, ao lançamento do MICROPROCESSADOR INTEL: "chip" 8085, com tecnologia de **8 bits** em escala comercial. O lançamento do micro APPLE II revoluciona a micro-informática; os micros a partir de então começam a ocupar seus lugares nas empresas.

A IBM, no início dessa década lança a família 370 e no fim da referida década a família 4341.

Uma pequena pastilha de silício, chamada microprocessador, do tamanho aproximado ao da cabeça de um lápis, é a grande responsável pelo avanço tecnológico do computador pessoal.

O primeiro microprocessador ou "chips" da linha 8088 possuía 5.500 transistores. Mais tarde surgiram os "chips" de **16 bits** da linha 80286, 134.000 transistores. Atualmente já estão em uso os "chips" 80386 e 80486 da INTEL, com **32 bits**, nas mesmas condições de tamanho, ou seja, a de uma cabeça de um lápis.

As gerações de computadores

Primeira geração - 1950/58

Caracterizaram-se por muito grandes e muito pesados, programados por painéis de chaves externas, 300 vezes mais rápido, que as fórmulas de cálculos convencionais, grande consumo de energia, apresentavam problemas de refrigeração, causando fusão de fios e queimas de válvulas, velocidade processamento da ordem de milissegundos e capacidade de memória de 2 a 4 kbytes.

Segunda geração 1958/65

Caraterizavam-se pela substituição das válvulas por diodos e transistores, menores e mais leves, programação interna, velocidade de processamento em microssegundos, 20 mbytes de memória; surgem os primeiros armazenadores externos: discos e fitas magnéticas.

Terceira geração 1965/75

Caracterizavam-se por ainda menores e mais leves, circuitos monolíticos integrados, avançados sistemas operacionais, velocidade de processamento em nonossegundos, multiprogramação, multiprocessamento e teleprocessamento, linguagens múltiplas de programação (COBOL, PASCAL, FORTRAN, BASIC, e outras).

Quarta geração - 1975.....

Caracterizam-se por circuitos integrados em longa escala, LSI - (Largue Scale Integration), produzidos pela INTEL, o primeiro microprocessador, rede de computadores, bancos de dados, computação distribuída, automação, micro-computador(microprocessador + memória + conversores + fonte de alimentação, tudo em um só móvel, os PCs).

Divisões

Computadores analógicos

Um computador analógico representa quantidades, através de grandezas físicas, realizando operações por meio de fenômenos físicos e dá resultados sob forma de números, sempre aproximados, não exatos. São usados em laboratórios de pesquisas e para publicações científicas e tecnológicas.

O computador digital representa quantidades por símbolos, executando operações através de meios matemáticos. Os resultados exatos, representados por caracteres (algarismos e letras) . são utilizados em organizações bancárias, comerciais, industriais, governamentais, etc.

O computador analógico realiza medições e o computador digital realiza cálculos.

Computadores de pequeno, médio e grande porte

Para esta classificação, leva-se em conta a capacidade de processamento do sistema, ou seja, a capacidade de armazenamento de sua memória interna. Pode-se assim classificá-los: pequeno porte com memória inferior a 32 mbytes, médio porte de 32 a 216 mbytes e de grande porte os com memória superior a 216 mbytes.

Diferença entre processamento de dados e processamento eletrônico de dados

Processamento de dados

Consiste em transformar determinadas informações, a fim de obter outras informações ou as mesmas informações sob outra forma, para algum objetivo, v. g., cálculo matemático, controle de estoque manual, contabilidade mensal.

Processamento eletrônico de dados

O sistema de processamento eletrônico de dados é definido como uma máquina ou um conjunto de máquinas, que executam o processamento de dados automaticamente.

Os sistemas cuja operação são realizados por circuitos eletrônicos recebe o nome de Sistema Eletrônico de Processamento de Dados ou Computador Eletrônico.

CRIMES DE INFORMÁTICA (II)

Direito de Informática

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)

O amoldamento do Direito à Informática, muito antes de individualizar-se no Direito Criminal, passa, necessariamente, por uma ótica mais ampla, mais geral. Essa ótica deve-se a o surgimento de limites especiais que impulsionam a um novo ramo do direito, que, a princípio, denomina-se Direito da Informática.

Tal constatação emerge da informatização da sociedade pós-industrial e, dela tornou-se dependente, sendo, pois, essa dependência que faz do computador um instrumento tão especial.

Ainda, essa dependência manifesta-se inquestionável, por exemplo, aos números elevadíssimos expostos no Brasil pelo Departamento de Comércio Exterior do Ministério da Fazenda e pelo Banco Central, que têm suas atividades vinculadas à própria existência dos computadores e sistemas.

Para se ter uma idéia da dimensão dos computadores na sociedade, a MICROSOFT, *"software-house"* mundialmente famosa, hoje, completa números como 60 milhões de cópias vendidas do seu WINDOWS nas versões 3.1 e 3.11, e, ainda espera números superiores para o recente lançamento que é o WINDOWS 95 (NEGROPONTE, jul,1995, p.7). Estes números referem-se a cópias regularmente vendidas, sem contabilizar a utilização de cópias pirateadas que rodam em computadores, e que estima que sejam perto de 2/3 das cópias vendidas. Assim, para dimensionar a elevada utilização desse *"software"*, os maiores eventos transmitidos mundialmente pela televisão jamais ultrapassaram a casa dos 55 milhões de espectadores.

Com esta visão genérica, o Direito Criminal da Informática deve ser desenvolvido com extrema rapidez e segurança, de modo a serem sistematizadas normas que atinjam os crimes empiricamente tipificados, que são cometidos com o emprego de computadores e sistemas, desenvolvendo proteção à privacidade, a instrumentalização da produção de provas, inclusive reciclando os conceitos de provas, principalmente aquelas provas técnicas. Tais iniciais parâmetros, ao nosso entender, são importantes para que se amplie a própria incipiente ciência do Direito

Criminal da Informática, com a abertura da exata compreensão do que representa o computador na vida de cada um, e, como tal, os riscos do avanço dos *crimes de informática*.

Até porque o legislador ao elaborar o Código Penal (1940), justamente a Parte Especial, visou o bem a ser protegido, tal como a vida, nos atentados contra à vida.

Nesse caminho, trilhado pelo legislador de 1940, é que deve espelhar-se o legislador brasileiro do fim do segundo milênio. Já que existe, no mundo dos fatos, sobejos elementos indicadores de *crimes de informática*, deve o legislativo nacional, redigir o Direito Criminal Brasileiro de Informática.

Assim, é seguro afirmar que estamos vivendo a primeira fase de um novo direito, o Direito Criminal de Informática. Devendo, pois, o legislador pátrio extirpar este, ainda que efervescente na cabeça e nos rabiscos de nossos doutrinadores, e transformá-lo em um Direito - com direito à maioridade - portanto, codificando-o em lei.

Generalidades

O Direito de Informática é rico em terminolgia e peculiaridades capazes de tornar-se quase uma ciência díspar do estudo do direito. Essa afirmação vem lastreada na riqueza de terminologia da ciência de informática e, quando aliado o seu estudo ao direito temos um vocabulário elevadamente rico. Portanto, mister se faz que a priori sejam exorcizados os termos mais freqüentes, de modo a garantir a clareza dos propósitos desta obra.

Programa

É uma seqüência de instruções em uma linguagem, que faz o computador realizar determinada ou determinadas tarefas.

"Software"

É um conjunto de programas, procedimentos e de documentação relativa à operação de um sistema de processamento de dados.

"Hardware"

São as partes eletrônicas e mecânicas, individualizadas ou em conjunto, de um sistema de computador. Como exemplo: o vídeo, o teclado, o mouse, a impressora, etc., são componentes de *"hardware"*.

"Chip"

É o um circuito integrado, montado, normalmente em uma pastilha ou plaqueta de silício.

Dado

Inicialmente, deve ser definido o termo DADO, que 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 e armazenado por um computador ou parte integrante de um computador. Ou, ainda, uma informação preparada para ser processada, operada e transmitida por um sistema de computador ou programa de computador. Os dados podem expressar fatos, coisas certas, ou comandos e instruções.

Os dados quando referidos em relação aos sistemas de computadores ou de comunicação constituam objetos tangíveis, objetivos, porque estão, ainda que de forma muito tênue, individualizados, através de orifícios microscópicos e áreas lisas com propriedades reflexivas diferentes no caso da tecnologia digital; não deixam de sê-los, atendendo-se, assim, as suas próprias características de dados de uma

informação. Portanto, os dados servem de suporte dos objetos imateriais, subjetivos que são as informações.

Informação

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 conhecimento.

Para o computador todo o dado é uma informação, quer como registro, quer como instrução, respectivamente, fim e meio, mas para nós, operadores do Direito, só certos dados ou grupos de dados constituem uma informação que poderá ou não formar ou ser parte de um tipo de conhecimento. Tanto o dado quanto a informação não são adventos da sociedade pós-industrial. A informação sempre foi muito valorizada, constituindo verdadeira forma e fonte de poder, seu controle.

É, portanto, que se acolhe o entendimento milenar de que os dados, dispostos como informação, ou seja, compilados, são um patrimônio econômico, político e cultural, que carregam potencial perigo, à medida que se tornam instrumento de poder e controle.

A automatização modificou a informação, dando à informação importância ao seu manuseio e controle, principalmente, quando se observa que é um fator que desenvolve e transmuda sem a intervenção do homem e operacionaliza através de métodos e processos automatizados.

Os números elevados de dados se transformam em informações de quantidade extraordinárias, chegam a um ponto que esta quantidade, ao seu manuseio, necessita ser qualificada. A qualificação surge com a informática, modificando a estrutura da informação e o seu fim. Neste ponto a informação automatizada, processada e operada pela informática aporta no Direito.

Dado/informação - a dicotomia

Quando coletados os dados, quantificados, preparados, sistematizados e compilados em um sistema de computador, passa, então, a ser um lastro de riqueza, de poder, de conhecimento.

Ambos, dados e informação, uma vez que têm sua importância maximizada na sociedade informatizada, tem que receber a proteção do Estado, através de legislação criminal, sob todos os aspectos.

Contudo, não se deve perder, concomitantemente, a diferença entre dado e informação.
Dado, no âmbito dos *crimes de informática*, deve ser utilizado, por ser mais palpável e objetivo. Enquanto que informação tem a textura flexível, não devendo ser utilizada na legislação penal.

A legislação penal, em qualquer tempo e espaço, deve abranger a forma mais simples inteligível ao computador, bem como ao ser humano, qual seja, o computador recebe dados e os processa. Assim, deve a legislação abranger essa idéia e dela derivar seus dispositivos de proteção.

As redes informatizadas

Atualmente, o homem médio, vê-se às voltas com o computador de várias formas, desde os serviços mais simples aos mais complexos.

O sistema de crédito eletrônico, por exemplo, nada mais é do que computadores ligados entre si, que formam uma rede, que se auto-sustenta, e têm alimentação de dados e/ou informações simultâneas, pelo acesso de um a todos e vice-versa.

Os grandes centros financeiros do mundo, não existiriam na complexibilidade, versatilidade e velocidade se não fosse o advento das redes de computadores. Esses, embora não constituam em si mesmo, um bem jurídico, podem ser descritos como um recurso disponível, proveniente da utilização de sistemas de computadores, programas, bases de dados e sistemas de comunicação.

Esse novo meio proporcionado pela moderna tecnologia é , na sua essência, um conjunto de recursos que se unem através de diferentes sistema de computadores, que oferecem garantia, rapidez e segurança nas operações que realizam.

Ao Direito Criminal de Informática interessam as redes de computadores, pois são constantemente alvos dos *crimes de informática*, porque, devido a sua complexibilidade, permitem ações que causam prejuízos imensos e, em razão da sua dimensão, dificultam a identificação do criminoso.

INTERNET

O que de mais moderno existe em informática é a INTERNET. Para acessá-la bastam um computador, um modem de transmissão, uma linha telefônica comum e um programa de comunicação.

A INTERNET é a maior rede de computadores do mundo e uma poderosa ferramenta de comunicação. Tem cerca de 35 a 40 milhões de usuários. Esta rede iniciou como meio de comunicação entre as unidades acadêmicas nos EE. UU., e depois se espalhou pelo mundo todo. Hoje, dentro de um gigantesco mundo virtual criado nas malhas da rede encontra-se de tudo, e é composta por: CYBERESPAÇO ("Cyberspace") que é o mundo virtual criado pela própria INTERNET. Nesse mundo existem *servidores* e *usuários* em 150 países e a conexão entre esses elementos é imediata e *"on--line"*; CORREIO ELETRÔNICO (*"e-mail"*) que é a correspondência que se pode enviar e receber diretamente pelo computador. O *"e-mail"* pode não ser tão pessoal quanto um bilhete à mão, mas se constitui na forma mais conveniente e rápida de comunicação escrita; ENDEREÇO ELETRÔNICO serve para enviar uma correspondência pelo computador, pois é necessário saber o endereço eletrônico do destinatário; *"HOME PAGE"* é a página principal de um serviço na *"World Wide Web (WWW)*; *"INFORMATION SUPERHIGWAY"* é a superestrada da informação. Neste caminho trafegam informação e imagem, e, em breve, até mesmo fitas de vídeo entrarão nas casas pela via eletrônica. Nesta superestrada, computadores, telefones, aparelhos de televisão e videocassetes viram um único *super-eletrodoméstico*; NAVEGADORES são os programas gráficos usados para se deslocar dentro da INTERNET.

O agente ativo - o delinqüente de informática

É de se supor que os *crimes de informática* são perpetrados por especialistas, *"expert"*, o que, hoje, é um engano, pois com a multiplicação de equipamentos, tecnologia, acessibilidade e, principalmente, os sistemas disponíveis, qualquer pessoa pode ser autor de *crime de informática*, bastando conhecimentos rudimentares de computação, para ser capaz de cometê-los.

Na década de 70, nos EE. UU., muitos delinqüentes de informática, após serem condenados a penas leves, eram contratados como especialistas em segurança e consultores de informática.

Em razão da popularização e simplificação do acesso aos computadores e pela redução dos preços de *"software"* e *"hardware"*, uma pessoa com o mínimo de

conhecimento é potencialmente capaz de cometer um *crime de informática*.

Hoje, através das inumeráveis compilações que circulam pelo mundo da informática, são os crimes dessa espécie cometidos à égide da ***"special opportunuty crimes"***, qual sejam, os crimes afeitos à oportunidade, perpetrados por agentes que têm a sua ocupação profissional ao manuseio de computadores e sistemas, em várias atividades humanas, e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores.

Essas compilações ainda trazem o perfil do delinqüente de informática, que são pessoas inteligentes, gentis, educados, principalmente, nos EE. UU. e na Alemanha, com idade entre 24 e 33 anos.

Agregam a esses, pela proliferação e popularização dos computadores e meios de comunicações através deles, a faixa etária entre 12 e 16 anos, principalmente nos EE. UU..

São todos, em regra, do sexo masculino, operadores competentes de computadores e sistemas, educados, brancos, dedicados, com "QI" acima da média. Devida a essa inteligência, geralmente privilegiada, são aventureiros, audaciosos e mantém com o computador e os sistemas um desafio constante de superação e de conhecimento. Para muitos é sua principal razão para trabalharem.

Têm, nesse desafio, sempre, a disputa, tanto com a máquina e seus elementos, como com os amigos que faz nesse meio, basta ver que os *crimes de informática* são perpetrados em co-autoria.

Entendem, exclusivamente ao seu juízo, não estarem cometendo qualquer delito, pois o espírito de aventura, audácia e de disputa bloqueiam seus parâmetros para avaliarem o legal do ilegal.

Suas condutas delituosas passam por estágios de objetivos. No início trata-se apenas de vencer a máquina. Após percebem que podem ganhar dinheiro extra. E , por fim, em razão desse dinheiro extra, passam a fazê-lo para sustentarem os seus altos gastos que são, em regra, com aparência pessoal e equipamentos de ponta na área de informática.

A esse perfil agrega-se o de serem pessoas avessas à violência e jamais incomodam-se de prorrogarem seus horários, inclusive, até gratuitamente.

Esse, em suma é o delinqüente de informática, que em qualquer parte do mundo mantém esse perfil, que dificulta ao máximo que seja surpreendido em ação delituosa, ou que se suspeite dele.

Denominação e conceito

O tema proposto e apreciado, *crimes de informática*, tem recebido denominações diversas em vários países, para designar as várias possibilidades de ações delituosas.

Os tratadistas da matéria como Aaron KOHN intitula Criminosos do Computador no seu editorial *"The Journal of Criminal Law, Criminoly and Policy Science"*, (apud FERREIRA, 1992, p. 140), utiliza *"Computer Criminals"*, para designar seus praticantes.

Jean PRADEL e Cristian FEULIARD referem-se a *"As infrações cometidas por meio de computador"* (apud FERREIRA, 1992, p. 141).

Klaus TIEDEMANN, (FERREIRA, 1992, p.142), porém, fala em *"criminalidade de informática"*, para designar todas as formas de comportamento ilegais, ou de outro modo prejudiciais à sociedade, que se realizam pela utilização de um computador. Nesse conceito Tiedemann engloba, por um lado, os problemas da esfera privada do indivíduo que possa ser ameaçada pela memorização, interconexão e transmissão informática de dados, e, por outro lado, os atentados ao patrimônio cometidos através de computadores e/ou sistemas.

A natureza dos delitos de informática, a complexidade e, principalmente, a ausência de unanimidade dos doutrinadores, fazem a dificuldade de definir os *crimes de informática*.

Martin WASIK, (*apud* Otto Banho LICKS e João Marcelo de Araújo Júnior, 1994, p. 95), sustenta que o *crime de informática* é um tópico difícil e onde não é fácil haver um consenso sobre a sua definição, não constituindo uma categoria legal precisa.

Valdir SZNICH (1992, p.3) define o *crime de informática* como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática que é essencial para a sua execução, investigação e acusação.

Em compilar tantos outros doutrinadores, ainda assim, não teremos abrangido o todo que compõe o *crime de informática*; o que se pode é englobar em uma definição genérica, pois é de ser considerado que não somente as características do fato punível, como, também, as peculiaridades da conduta e os traços do caráter e da personalidade do seu autor.

É, pois, nesta esteira que se define o *crime de informática* pelo que caracteriza a conduta lesiva, a qual não necessita corresponder à obtenção de uma vantagem ilícita. Por oportuno, é de ser ressaltado que não se incluem aquelas condutas que caracterizam crimes tradicionais, que têm por objeto material os sistemas de computação, seus componentes ou *"software"*, tal como o furto de *"hardware"* ou

"software". Assim, quem subtrai um computador com ânimo de vendê-lo, não estará cometendo um *crime de informática*.

Por exemplo, o jornal ZERO HORA, (Porto Alegre, 16,ago,1995) em seu Caderno De Informática, publica matéria sob o título *"Aumentam os Roubos de Chips"*, no qual descreve que criminosos entraram no prédio da British Telecom, a companhia telefônica britânica, abriram 200 computadores e levaram apenas os *"chips"*. Vê-se, pois, que não é "*crime de informática*", embora para tal execução exija do delinqüente conhecimento rudimentar de *"hardware"*. É', assim, um delito comum, entre nós, de furto qualificado.

Ao nosso entender grande parte da doutrina, define o *crime de informática* pelo bem jurídico protegido. É a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar.

Isto posto, depreende-se que o *crime de informática* é todo aquele procedimento que atenta contra os dados , que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão.

Assim, o *crime de informática* pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador utilizando-se *"software"* e *"hardware"*, para perpetrá-los.

Conclui-se que aquele que ateia fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, não comete *crime de informática*, do mesmo modo, aquele que, utilizando-se de computador, emana ordem a outros equipamentos e cause, por exemplo, a morte de alguém. Estará cometendo homicídio e, não *crime de informática*.

A polêmica é, verdadeiramente, grande e a terminologia não é pacífica. Para demonstrar isso encontramos *"Criminalidade Mediante Computadores", "Criminalidade do Computador", "Delito Informático", Criminalidade na Informática", "Crimes Cometidos Pelo Computador", "Crimes de Informática"*, entre outros.

Seja qual for, porém, a denominação que lhes é atribuída, essas ações criminosas identificam-se, na diversidade de suas classificações, pelo seu objeto ou por seus meios de atuação, que lhes fornecem um denominador comum. E, assim atesta a definição proposta pela Organização para a Cooperação Econômica e Desenvolvimento orienta a qual (*apud* FERREIRA, 1992, p. 141) que: "O *crime de informática* , ou **computer crime** é qualquer conduta ilegal não ética, ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados".

Neste trabalho preferimos utilizar a expressão *crimes de informática*, entendido como tal, toda a ação típica, antijurídica culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão.

Este conceito, que se coaduna com a Teoria Penal vigente no Direito Penal Brasileiro, pouco difere do adotado pelo Conselho da Europa e Comunidades Européias, porém, caracteriza melhor os elementos necessários para a criminalização da condutas puníveis.

Semanticamente, o conceito de ação abrange qualquer comportamento humano, positivo ou negativo, desde que seja típico, ou seja, corresponda ao modelo previsto na lei como crime, com a penalidade respectiva, atendendo-se ao princípio *"nullum crimen nulla poena sine lege"*, que é básico em nosso Direito.

Atendido o princípio da legalidade, o conceito de crime se completará se a conduta for ilícita e a responsabilidade penal puder ser atribuída ao seu autor pelas características que compõem a culpabilidade e que são a imputabilidade penal e a consciência potencial da ilicitude, sendo exigível dele um comportamento conforme o Direito.

Nos *crimes de informática*, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

CRIMES DE INFORMÁTICA (III)

Direito Penal de Informática

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)

Face ao espaço considerável que ocupa na vida cotidiana, a informática apresenta-se no Brasil como na maioria dos países, como um fator dos mais relevantes nas relações econômicas e sociais e, conseqüentemente, nas relações jurídicas de qualquer natureza, sejam elas cíveis, administrativas, comerciais, etc.

Henry BOLSOY aponta (apud FERREIRA, 1992, p.143) três ordens de relações da informática com o Direito Penal:

- ***"a) a informatização da documentação penal"***, que compreende o famoso fichário policial e os arquivos judiciários e dos serviços de segurança, contra os quais muitas vezes se faz necessário reforçar as medidas de proteção e as garantias individuais pela excessiva ou leviana intromissão dos órgãos estatais na vida privada dos cidadãos.

  Nesse sentido a Constituição Federal Brasileira, de 05 de outubro de 1988, temos:

  "conceder-se-á habeas data:

  a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes nos 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."

  Essa garantia constitucional visa a prevenir que atos dos órgãos públicos, baseados em informações sigilosas, permaneçam ignorados pelo interessado, que ficaria assim impedido de qualquer defesa ou objeção.

- ***"b) a informação dos procedimentos administrativos e processuais"***, melhorando e aperfeiçoando a distribuição da justiça, aliviando os trabalhos judiciários e facilitando o cumprimento das sentenças e execuções penais.

  Os órgãos da Justiça Penal Brasileira, principalmente de grandes centros urbanos, vêm-se se modernizando e se aparelhando com o processamento automático de dados, o qual , mais do que uma conveniência, tornou-se uma necessidade imperiosa ante ao grande volume de processos que superlotam os nosso tribunais e, na área penal, pela facilidade que esse procedimento representa para a correta informação sobre antecedentes dos acusados, por exemplo.

- ***"c)a informática a serviço da delinqüência"***, permitindo-se falar em infrações favorecidas pela informática.

  Esses *crimes de informática* ora apresentam apenas novas maneiras de executar as figuras delituosas tradicionais, ora apresentam aspectos pouco conhecidos, que não se adaptam às incriminações convencionais e seus autores aos tipos criminosos comuns.

Uma das exteriorizações mais freqüentes é a fraude praticada com diferentes formas de manipulação de dados e programas ou utilização abusiva do computador. Mas, também, o furto, a apropriação indébita, o vandalismo, causando consideráveis prejuízos patrimoniais, são formas comuns de abuso da informática, além de que, são realizados na área do Direito Penal Econômico (crimes do colarinho branco), ou contra a liberdade individual (violações da intimidade ou sigilo das comunicações, ou, na área do direito do autor ou da proteção de marcas de indústria e comércio (sabotagem ou espionagem industrial).

De outra banda, inúmeros problemas e grandes prejuízos podem ser causados pelas ações praticadas contra o funcionamento da própria máquina, como é o caso dos disseminação proposital do chamado **VÍRUS** do computador, destruindo programas fichários do usuário e, o caso mais recente, que teve repercussão em todos os meios de comunicação do mundo, foi a ação do vírus HIROSHIMA 50 ANOS, que atacou os computadores do Hipódromo da Gávea, quando da realização do Grande Prêmio Brasil, causando prejuízos de grande monta, e tal ação criminosa foi atribuída ao grupo ecológico internacional "GREENPEACE".

E quais dessas condutas têm relação com o Direito Penal?

Duas grandes fendas emergem de pronto: por um angulo a tipificação dessas condutas que se inserem em razão do meios empregados e seus agentes o *"white collar crim"* (crime do colarinho branco).

De outro a complexidade dos sistemas de computadores e eles próprios, que dificultam a que se descubra o golpe, como impedem que as raras provas cheguem à Justiça.

Aqueles que tratam do Direito Penal, qualquer que for a fase (policial ou judicial) têm profundas dificuldades em consolidar provas capazes de, até, iniciar um inquérito policial, quiçá oferecer denúncia.

Para se ter a idéia dessa complexidade e da própria dificuldade em aplicar o direito vigente, Valdir SZNICH (1992, p.15) alenta a hipótese de que:

"o agente dá uma ordem ao computador - dentro da programação - repete realizando-se, espaçadamente, a mesma operação. Tem-se inicialmente o que se chama delito à distância, mas que para a doutrina penalista de pouca valia tem para o agente. No caso citado o agente realiza uma conduta delituosa e, dada a programação, de tempos em tempos essa mesma conduta se repete. Que espécie de infração temos aí? Crime instantâneo de efeitos permanentes, crime permanente ou continuado?"

Como se vê, para tal solução tem ser apurado o meio, a localização do agente, o meio empregado, o objetivo, o resultado e os efeitos do resultado, sem falar que emerge, necessariamente, a questão da competência. Para tanto, digamos que o agente estivesse em uma cidade e o resultado foi alcançado em outra e o lesado, ainda, em cidade distinta de ambas.

Tal delito, seguramente, trará problemas de ordem jurídica material e processual, portanto, temos como improrrogável ser escrito o Direito Criminal Brasileiro de Informática.

OS SISTEMAS DE CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

Diversas classificações são propostas para ordenar o estudo da matéria, sendo mais comuns os que se baseiam na distinção entre os crimes tradicionais, pela utilização da informática, e , noutra categoria, as outras ações de abuso de informática, específicos dessa área.

Essa é, exemplificando, a classificação de Ivete Senise FERREIRA (1992, 9. 147), que se baseia no trabalho de Martine BRIAT, que distingue:

- manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;

- falsificação de dados ou programas;

- deteriorização de dados e programas, e entrave à sua utilização;

- divulgação, utilização ou reprodução ilícitas de dados e programas;

- uso não autorizado de sistema de informática;

- acesso não autorizado a sistema de informática.

Ivete Senise FERREIRA, preferiu em sua classificação, não fazer menção aos computadores nem os seus elementos técnicos, os quais podem sofrer modificações muito rápidas pelo avanço da tecnologia neste setor.

Outras pessoas pensam de modo diferente, como Marc JAEGER (1985, p.23) que, além de preferir o termo *fraude informática*, tomado no sentido lato, para designar todos os ilícitos penais ou ações repreensíveis ligadas à informática, distingue nelas duas categorias apenas:

- fraudes propriamente ditas;

- atentado à vida privada.

Todavia, existia a possibilidade de, na prática, várias dessas ações se misturarem, e com esse entendimento propõe Hermann Cohem JEHORAM (1991, p. 278) para as fraudes uma classificação que se baseia no próprio equipamento utilizado:

- fraudes no nível da matéria corporal ou do *"hardware"*, ou seja, contra a integridade física do computador;

- fraude ao nível do input, ou seja, na entrada de dados;

- fraudes ao nível do tratamento dos dados, ou seja, modificação apenas dos programas, sem atingir os dados;

- fraudes ao nível do output, ou seja, intervenção no resultado obtido a partir de dados corretos, corretamente tratados.

Muitos doutrinadores, porém, baseiam-se na finalidade visada pelo autor do delito para classificá-lo, que envolvem os *crimes de informática* aqueles que se enquadram no Código Penal ou aqueles que não são cometidos por meio de computador, mas, sim, por ocasião da utilização dele, e depois distinguem duas características:

a) manipulações para obtenção de dinheiro, em sentido do proveito econômico;

b) manipulações para obtenção de informações de forma individual, ou seja, não teria direito.

Essas inúmeras outras classificações constituem uma tentativa para analisar a complexidade das situações que na prática podem surgir com a utilização abusiva da informação, bem como medidas legais para evitá-las.

Também, por peculiares, transcrevemos a classificação de Hervé GROZE e Yves BISMUTH, (1986, p. 207);

- os atos dirigidos contra um sistema de informática, por qualquer motivo;

- os atos que atentam contra outros valores sociais de um sistema de informática.

Na primeira categoria, que constitui o verdadeiro núcleo da delinqüência informática, segundo GROZE e BISMUTH, situam-se os variados componentes que atentam contra o material, seja contra os suportes lógicos ou dados do computador.

Na segunda categoria, pode-se dizer que cabem todas as espécies de infrações previstas nas leis penais, lembrando que ao nosso entender não é delito de informática, pois os meios da informática são meros instrumentos de delitos comuns, como o exemplo já citado, daquele que por meio de um computador emana instruções para matar alguém. Não estará cometendo um *crime de informática*, e,

sim, um homicídio, artigo 121, *"caput"*, do Código Penal.

Não obstante as classificações elencadas, entendemos que os *crimes de informática* dever ser classificados quanto ao seu objetivo material, a saber:

- **Crime de Informática Puro**

São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o *"software"*, o *"hardware"* (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.

Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo.

As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador.

Portanto, é *crime de informática* puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

- **Crime de Informática Misto**

São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

Quando o agente objetiva, por exemplo, realizar operações de transferência ilícita de valores de outrem, em um determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um *crime de informática* misto.

É *crime de informática* misto porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas

(art. 70, CP).

- **Crime de Informática Comum**

São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo agente ativo, que poderia escolher outros meios diversos da informática. Porém, é de se pensar na possibilidade de qualificadora para o delito de estelionato o uso do sistema de informática.

Despiciendo aclarar a aplicabilidade aos crimes comuns das normas penais vigentes, porém, poder-se-ia, atendendo a essa classificação, incorporar ao Código Penal agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito.

Posto isto, entendemos ser a presente classificação apta a elaboração de legislação que possa alcançar os delitos de informática, sem contudo, correr-se o risco de sobreposição de normas, e, assim, também, entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

CRIMES DE INFORMÁTICA E SEUS OBJETIVOS

Antes mesmo da classificação dos *crimes de informática*, é de ser avaliados e analisados os bens cuja proteção devem ser objeto do ordenamento jurídico vigente, ou através de novos tipos específicos.

Existe ainda hoje uma bipolarização em torno de que bem jurídico é fundamentalmente protegido pelo Direito Penal de Informática, se os sistemas ou se as informações.

O Organização para a Cooperação Econômica e Desenvolvimento, FERREIRA, 1992, p. 141., apesar de definir de forma ampla os delitos de informática, é favorável à proteção da informação, embasada na importância das informações na sociedade pós-industrial.

O National Center For Computer Crime Data, dos EE. UU., (*apud* LICKS e ARAÚJO, 1994, p. 89) defende a posição de que o Direito Criminal de Informática é concebido para proteger os sistemas de computadores e das comunicações, além da informação.

Deve, assim, ser entendido, 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 dados, e os dados que ainda não contam com a mesma proteção do outro componente, o *"hardware"*.

Embora a distinção entre *"hardware"* e *"software"* seja pacífica do ponto de vista técnico 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 bem como os bens materiais.

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

Neste ponto, por oportuno, deve ser aberto um nicho de informação, no que tange ao direito sobre propriedade imaterial, mais precisamente o Direito do Autor.

A obra criada por computador é uma forma tornada possível pela técnica da informática e que se amplifica com os modernos sistemas de inteligência artificial.

Mas logo surge quem pretenda atribuir-se direitos exclusivos em relação a essa obra; e mais quem pretenda que a tutela seja outorgada pelo Direito do Autor. Assim, já a lei inglesa de 1988, na sua seção 178, prevê que para as obras geradas em circunstâncias não há autor humano; mas, paradoxalmente, considera autor a pessoa por quem foram empreendidas às disposições (*"arrangements"*) necessárias para a criação da obra. Em última análise, acaba por beneficiar o produtor. Também no Japão, o dono da máquina é dono de tudo o que ela produz.

Em Portugal, porém, nenhuma proteção é admissível. Porque a obra criada por computador nem é objeto de proteção específica, nem cai em nenhum dos tipos existentes.

No Brasil, nessa área, especificamente, existe a Lei n. 5.988, de 14 de dezembro de 1973, que regula os direitos autorais, sem, contudo, qualquer dicotomia sobre minúcia da informática. É uma norma genérica. Em relação à informática, temos a *"Lei do Software"*, Lei n. 7.646, de 28 de outubro de 1987, que foi regulamentada pelo Decreto n. 96.036, de 12 de maio de 1988, que dá proteção jurídica somente ao *"software"*.

Tal fenda foi aberta para demonstrar o quanto é complexo esse novo direito que nasce, que é o Direito da Informática, e, para nós, o Direito Criminal da Informática.

Assim, 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 e a criação, protegidos pela propriedade intelectual foram durante muito tempo os únicos bens imateriais mensuráveis, aferíveis e protegidos pelo direito patrimonial, que eles são os únicos bens imateriais relevantes para o Direito, atualmente. É. pois, um instituto diferente da propriedade intelectual e o segredo de indústria ou de comércio, estes já respaldados por diversas legislações, onde o bem tutelado é essencialmente uma informação ou conhecimento, e não a 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 como nas legislações.

O computador vem trazer novos desafios para os crimes já previstos nestas três modalidades de entendimento, através de formas quanto ao meio de cometimento de tais delitos. A detecção e a efetiva acusação de crimes já tipificados nos crimes em que se utiliza o computador torna-se maior o grau de reprovabilidade da conduta face ao maior dano causado por crimes contra tais bens empregando-se a informática, bem como o necessário elevado nível intelectual do delituoso.

O computador é usado para a prática de um delito, do mesmo modo que outros artefatos. Discute-se, então, a criminalização de tais meios de cometimento, visto que certos crimes se tornam quase impossíveis de tipificar, provar e processar quando praticados no ambiente informático.

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 das transformações sofridas pela sociedade pós-industrial, com o impacto causado pela moderna tecnologia da informação.

CRIMES DE INFORMÁTICA (IV)

Crimes em Espécie - Comuns e de Informática

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)

Por muito importante, é não ter sido, ainda, pacificada a proteção do bem jurídico, face às imensuráveis divergências entre os grandes doutrinadores.

Acima citamos o furto de *"chips"* da Britsh Telecom, e ao primeiro impacto pode-se tratar de crime comum, pois a conduta não teria as duas premissas fundamentais dos "*crimes de informática*", quais sejam, o objetivo dos dados ou sistema, perpetrados através de computador.

Dada a importância do *"chips"* é que o professor da Universidade de Amsterdã, Hermann Cohen JEHORAM (1991, p. 277), fez publicar o artigo "Proteção do Chip", no qual inicia perguntando: *"Chips podem ser comparados com qualquer outro objeto de proteção da propriedade intelectual?"*

É de ser respondido que em literatura desatualizada, e esta evolui na mesma velocidade do avanço tecnológico dos computadores, sistemas e periféricos, encontram-se, com freqüência, tropeços na comparação de *"chips"* com *"software"*. Como exemplo, se vê numa longa carta de 16.05.85 escrita pelo governo holandês à Comissão Americana de Patentes e Marcas Industriais. O então signatário queria provar que *"chips"* já eram protegidos pela lei dos direitos autorais, proteção que se dizia evidente a conta de decisões citadas, assegurando proteção ao *"software"*, a ele, por conseguinte extensivo ao *"chip"*.

A Associação entre *"chip"* e *"software"* de computador hoje em dia pode ser tecnicamente explicável, mas legalmente incorreta. *"software"* de computador é realmente *"software"* e, como tal, pode, no mínimo, ser comparado à obra literária, objeto clássico protegido pelo direito autoral. Não se considera neste contexto aquele misto de confusão e contradição, que hoje se diz ter havido nos EE. UU., quando a razão foi substituída pela euforia sobre a proteção do *"software"* como direito autoral.

"Chips", porém, são *"hardware"*, microcomputadores, portanto máquinas. Em realidade, não se reivindica proteção dessas máquinas como tais, mas como desenho, que é chamado nos EE. UU. MASK WORK; topografia de produto semicondutores no Mercado Comum europeu; e LAYOUT de circuito semicondutor integrado no Japão. O esboço de tratado preparado pela Organização Mundial de Proteção Industrial sobre o assunto é o mais claro quando fala de desenho de circuito integrado.

Desenhos podem ser protegidos pelo direito autoral? A resposta não pode ser universalmente dada como nos casos de obra literária e *"software"*. Não há, realmente, em todo o direito de propriedade intelectual nenhum assunto que suscite tanta divergência nos sistemas nacionais, como a proteção dos desenhos, no campo do direito autoral, pois não se enquadrando nesse, obrigatoriamente, deveria ser apreciado no campo do Direito Criminal da Informática, porque é um bem que se tem e deve ser protegido.

Portanto, indelével, as peculiaridades que cercam o computador, seus componentes e a própria informática, necessitando, urgentemente, os doutrinadores encontrarem parâmetros, meios capazes de escriturarem o Direito Criminal da Informática, de modo a garantirem proteção desses bens, que, também, são jurídicos, à medida que geram direito, de uma ou de outra forma.

Muitos têm escrito a cada conduta ilegal, com o intuito de classificarem que esta ou aquela conduta é passível de ser um *crime de informática*, ou não, porém, o segmento mais claro, que estabelece linha cristalina entre os delitos comuns e os delitos de informática, é aquela que define os *crimes de informática* nas condutas em que o agente ativo visa aos dados ou sistemas do computador e, utiliza-se como meio para alcançá-lo, o computador.

Contudo, os *crimes de informática* encontram do Código Penal Brasileiro várias possibilidades de repressão pena, variando a sua tipificação conforme o bem jurídico que o agente pretenda atingir.

CRIMES COMUNS

Considerações Gerais

Na nossa lei penal o patrimônio da pessoa física ou jurídica é tutelado pelo Código Penal, como também os crimes contra a divulgação de segredo. Todavia, observa-se que tais previsões legais podem e devem ser aplicadas às condutas que envolvem delitos de informática, principalmente naquelas em que o sistema de informática é ferramenta ou é alvo de delito comum, por isso, que buscamos na lei penal a possibilidade de tipificação de algumas condutas que envolvem o sistema de informática. Buscamos, a seguir, demonstrar a sua aplicabilidade aos delitos de informática, sem, conduto, aprofundar descrição e interpretação, pois, do contrário, estaríamos desvirtuando o objetivo deste trabalho.

Do Código Penal

FURTO

Objeto jurídico

O artigo 155 protege, inicialmente, a posse de *"hardware"* e *"software"*, para depois a propriedade. É de ser entendido que o furto de *"software"* é a subtração de sistema que esteja instalado no computador. O furto simples de equipamento e sistemas são crimes comuns contra o patrimônio e a propriedade.

Sujeito ativo

É todo aquele que se apossa por meio de subtração para si ou para outrem de *"hardware"* ou *"software"*, estejam eles na posse do proprietário ou na de terceiros. É aquele que tem na sua ação *"animus furandi"*.

Sujeito passivo

É toda a pessoa física ou jurídica que tenha a posse ou a propriedade de computador ou sistema de informática.

Ação física

É a ação de subtrair, surripiar do domínio do proprietário ou de quem tenha a posse de computador ou sistema de informática.

Objeto material

É o computador ou o sistema alheio, que se acha na posse de outrem, seja proprietário ou não. É admissível, assim, no uso desautorizado do computador o furto de energia elétrica, e este é previsto no Código Penal (art. 155, § 3o.), porém, neste caso, esbarra no valor irrisório ou do prejuízo ínfimo da vítima.

Devem ser excluídos os furtos de *"softwares"* com objetivo de *pirataria*, este delito é tratado através dos crimes contra a propriedade imaterial, e alguns entendem ser nos crimes contra a propriedade industrial.

O bem objeto de furto, além de ser alheio, deve ser móvel. O computador é, por sua natureza, um bem móvel, o *"software"* que nele estiver contido por via de conseqüência é também, neste caso, um bem móvel. Os dados armazenados são, também, coisa móvel, porém é de se perquirir se o agente visava o tão somente o equipamento, se visava exclusivamente o *"software"* ou aos dados. É *crime de informática* puro.

Elemento subjetivo

Não existe furto sem dolo. O agente sempre tem a intrínseca vontade livre e consciente de praticar o delito, de subtrair o equipamento, não há que se discutir a sua forma culposa.

Consumação e tentativa

A consumação do furto de computador ocorre quando o bem sai da esfera da posse da vítima, para entrar na do agente ativo, de forma mansa e pacífica. A tentativa é admissível.

Furto noturno

Atende ao que determina a lei penal, como agravante do delito de furto, plenamente caracterizável.

Qualificadoras

Admitem-se as qualificadoras de destruição ou rompimento de obstáculos à subtração da coisa, no caso em que o agente necessite, para perpetrar o furto de informações, abrir a caixa do computador e mudar o chaveamento, para anular a senha de acesso ao disco rígido, por exemplo.

Quanto ao abuso de confiança é perfeitamente perceptível, quando o agente é empregado da vítima. A fraude pode ocorrer na hipótese de que , para furtar informações a agente usa de meios que caracterizem a conduta fraudulenta, como, no caso de dizer-se técnico da empresa que fornece manutenção do equipamento.

A escalada e o uso de chave falsa, somente se o agente, para entrar no local onde se encontra o computador necessita usar de meios anormais.

O furto por destreza não se aplica aos *crimes de informática* em razão das suas características, tanto do objeto o furto, como do meio.

DANO

O artigo 163, nos casos em que o agente visa à destruição, inutilização ou deterioração da coisa alheia (o computador, os periféricos, as informações e os sistemas) são aplicáveis à informática, bem como as qualificadoras de violência à pessoa ou grave ameaça; com emprego de substância inflamável ou explosiva; contra patrimônio da União, Estado, Município, empresa de economia mista ou que seja concessionária de serviços públicos; por motivos egoísticos ou com prejuízo considerável à vítima. Nesse caso tem que perquirir o *"animus delinquendi"*.

Objeto jurídico

Concerne a tutela à inviolabilidade do patrimônio, aqui o computador, em razão de que o dano causado reduz ou suprime a utilização e o preço do computador.

Á informática concerne danos físicos ao computador na sua forma interna e externa. Se os danos visam à destruição do equipamento é aplicável, exclusivamente, o artigo 163 do Código Penal, porém, se os danos vão além da parte física do equipamento, atingindo *"software"* e dados, é de ser apurada a vontade do agente. Se visa ao *"software"* e/ou aos dados contidos no computador é crime puro de informática; contudo, não inviabiliza o concurso material.

Sujeito ativo

É todo aquele agente que visa causar dano ao equipamento de forma a causar prejuízo ao proprietário ou a quem tenha a posse dele. É importante ser buscada a vontade do agente, no caso, tem que ter tão somente o "animus dolandi"".

Sujeito passivo

É todo aquele que tem o uso e o gozo do equipamento.

Ação física

Forma comissiva, caracteriza-se quando o agente busca o dano através de ação idônea a atingir seu objetivo ilícito.

Na forma omissiva o agente permite que ocorra o dano ao equipamento, permitindo que ações outras visem a destruir, inutilizar ou deteriorar o equipamento.

Elemento subjetivo

Admite dolo e culpa. No dolo o agente tem a vontade consciente de alcançar o resultado dano. Na forma culposa, pratica ação arriscada que inutiliza, deteriora ou destrói o equipamento, por exemplo, danos causados ao disco rígido, por imprudência, por imperícia ou negligência.

Objeto material

Visa, tão somente ao *"hardware"*, não vislumbrando os danos de "*software*s" e das informações contidas no equipamento.

Consumação e tentativa

Admite, plenamente, a forma tentada na sua ampla concepção doutrinária, legal e jurisprudencial, bem como se consuma ao alcançar a destruição, deterioração ou inutilização do equipamento.

APROPRIAÇÃO INDÉBITA

O artigo 168 é uma das figuras típicas que é afeita aos *crimes de informática*. O agente, quase sempre, tem a posse ou detenção do equipamento, e dele se serve para perpetrar vários delitos de informática. Portanto agrega-se com propriedade a causa de aumento de pena se o delituoso age em razão de ofício, emprego ou profissão.

Objeto jurídico

É, também, delito que objetiva o patrimônio, aqui *"hardware"*. Atingindo com mais freqüência empregadores, sejam eles pessoa física ou jurídica.

Sujeito ativo

É todo agente que se apropria coisa de que tem em sua guarda. É comum nas relações de emprego e de confiança.

Sujeito passivo

Em princípio, qualquer pessoa que suporta o prejuízo pela apropriação indevida, podendo ser pessoa física ou jurídica.

Ação física

Ocorre após o agente ativo receber para guarda o *"hardware"*, de que após se apropria com o *"animus domini"*.

Objeto material

São todos os tipos de equipamentos que fazem parte do *"hardware"*, tais como, vídeo, unidade centra de processamento (CPU), mouse, impressoras, scanners, etc., porém inaplicável a informações sob a forma de dados ou o *"software"*.

Elemento subjetivo

Como qualquer crime, dessa natureza, requer a apropriação indébita, o dolo genérico, que constitui a vontade livre e consciente do agente em apropriar-se do equipamento, com a intenção de tê-lo para si.

É, no entanto, não é admissível a culpa na apropriação indébita, pois, no caso do agente apropriar-se do computador pensando ser seu, estará agindo ao impulso do erro de fato.

Consumação e tentativa

É difícil a caracterização da consumação. É necessário um profundo exame do elemento subjetivo combinado com os atos exteriorizados pelo agente, e, mesmo assim, nem sempre é possível captar-se a consumação.

A tentativa é matéria jamais pacificada, vez que alguns doutrinadores entendem impossível a tentativa; outros, pelo elemento subjetivo e os atos exteriores podem caracterizar a tentativa.

***"In casu"*, é de ser seguido a regra geral desposada pela lei penal, que determina o *"iter"* e a vontade do agente seja perceptível.**

ESTELIONATO

O artigo 171 é, também, um dos instrumentos que permite alcançar a agente de *crimes de informática*, porque o *"caput"* prevê, substancialmente muitas condutas desenvolvidas contra o computador e os seus sistemas. Os "*crimes de informática*", por enquanto, no artigo 171 o meio mais eficaz aplicar o Direito Penal, visto que, a abrangência das condutas tipificadas são perfeitamente enquadradas, na sua generalidades, a todos os tipos de condutas delitivas contra o computador, periféricos, sistemas e informações.

Sujeito ativo

É o agente que se locupleta com a vantagem ilícita, que se utiliza dos meios informáticos a induzir ou manter a vítima ou alguém em erro, é pois á regra.

Sujeito passivo

É a pessoa jurídica ou física que suporta o prejuízo pela ação delituosa.

Ação física

O que caracteriza o estelionato na informática é o meio fraudulento, o artifício, o ardil que é usado pelo agente ativo para atingir o patrimônio de outrem.

O computador, como meio fraudulento é, em nossos dias, uma ferramenta poderosa e eficiente nas mãos de delinqüentes que tenham conhecimento técnico, haja vista que, por exemplo, os maiores prejudicados por este tipo de delito tendo como ferramenta os meios informáticos, são as instituições financeiras.

A fraude eletrônica é, para muitos, o sinônimo de *crime de informática*, por isso, incontáveis são as formas físicas aptas a alcançar a consumação do delito de estelionato, pela via eletrônica.

Dolo

Requer o dolo genérico, ou seja, a vontade livre e consciente de praticar o fato punível e antijurídico.

Consumação e tentativa

Consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É, também, admissível na forma tentada, na sua amplitude conceitual, porém, é de ser buscado o meio utilizado pelo agente, vez que impunível o meio inidôneo.

Por outra, é de ser ressaltado o estelionato, que tem como ferramenta os meios informáticos, é de difícil coleta de provas, pois, os conceitos de admissibilidade dos meios informáticos como meio probante, são, ainda, insipientes em consolidá-los como meio hábil de prova. São necessárias muitas pesquisas e coleta de elementos circunstanciais para iniciar-se, até, o próprio inquérito policial.

DIVULGAÇÃO DE SEGREDO

A regra do artigo 153 (Código Penal) permite, de forma extensiva, se pode aplicar às ações que resultem em violação de segredo, coletados e captados por meio da informática, de forma desautorizada, e, principalmente, se produzirem danos à vítima.

Mesmo entendimento deve ser aplicado ao que se refere ao artigo 154 (Código Penal), o qual, ao nosso entender, nada mais seria do que uma causa de aumento de pena, referente ao artigo 153.

Tal entendimento exsurge, por exemplo, nos sedimentos da transmissões de mensagens via computador. Principalmente hoje, com o advento da grande infovia que é a INTERNET, vez que, o usuário tem endereço eletrônico, no qual recebe suas correspondências informatizadas.

Objeto material

É o documento ou a correspondência, seja ela na forma que for, pois a norma visa a proteger a liberdade individual, e assim, qualquer violação de meio físico de armazenamento de segredo tem que ser considerado como documento ou correspondência.

Sujeito ativo

É todo aquele agente que viola correspondência ou documento eletrônico, passando a divulgar segredo neles contidos.

Sujeito passivo

Aqui cabe ampliar o entendimento desposado pelo Código Penal. Como o delito se concretiza pela violação e divulgação de segredo, esta ação não só atinge o destinatário, como também, o remetente, pois o segredo pertence a ambos, e a sua divulgação prejudica aos dois. Por isso, pode ser pessoa física ou jurídica.

Ação física

É o ato de violar e revelar o conteúdo de documento ou correspondência eletrônica, desde que contenha segredo. Aplica-se quando o agente viola o computador visando os segredos armazenados nos acumuladores do equipamento, assim, pois, trata-se de um crime puro de informática.

Elemento subjetivo

É o dolo, a vontade consciente e livre de violar e divulgar o segredo contido em meios eletrônicos.

Elemento material subjetivo

No caso da informática, muitos segredos podem e são mantidos em arquivos de dados. Se violados e divulgados, ter-se-ia a aplicação dos artigos 153 e 154 do Código Penal, c/c a norma de informática penal própria, pois, entendemos, neste caso, um *crime de informática* puro, todos na forma do artigo 69 do Código Penal.

A Lei dos direitos autorais

Contra a propriedade intelectual

Os direitos autorais são regulados em nosso país pela Lei n. 5.988, de 14 de dezembro de 1973 e pela Lei n. 6.895, de 17 de dezembro de 1980. A primeira definindo direitos morais e patrimoniais do autor e a segunda adequando a violação de direito de autor à Convenção Internacional celebrada em Genebra em 29 de outubro de 1971 e promulgada no Brasil pelo Decreto 76.906, de 24 de dezembro de 1975.

Assim o artigo 184 do Código Penal, tem a redação dada pela Lei 6.895/80, portanto, aplicável aos *crimes de informática* que envolverem direitos autorais, principalmente nos crimes de pirataria, cópias de sistemas não autorizada.

Contra a propriedade industrial

Infrações típicas da área dos negócios, ou crimes do colarinho branco, não acarretam muitos processos penais, preferindo os interessados recorrer a acordo comerciais e indenizações na área civil. De um modo geral a propriedade industrial compreende o direito exclusivo do autor de uma descoberta ou de uma invenção de apropriar-se dela, o direito de uso exclusivo de marca de indústria ou comércio, desenho ou modelo, nome ou designação especial que distinga seus produtos de similares. Todos são passíveis de terem como meio o computador e seus sistemas.

O Código da Propriedade Industrial é a Lei n. 5.772, de 21 de dezembro de 1971, que conservou, em matéria criminal, os dispositivos da lei que veio substituir, o Decreto-lei n. 7.903, de 27 de agosto de 1945, que já previa essas infrações.

***A Lei do* "software"**

A Lei n. 7.646, de 18 de dezembro de 1987, denominada Lei de Informática, no seu artigo 2º declara que o regime de proteção à propriedade intelectual de programas de computador é o direito do autor - Lei n. 5.988, de 12 de dezembro de 1973, mas com as modificações que estabelece para atender às peculiaridades inerentes aos programas de computador.

Um problema agregado a este assunto são as leis que protegem a propriedade intelectual é que vão se tornando obsoletas em razão das novas formas de "pirataria".

A indústria do *"software"* é um dos negócios mais rendosos da atualidade, com um mercado global de mais de 77 milhões de dólares no ano de 1994, segundo dados do Departamento de Comércio dos EUA. Na maioria dos países, o número de computadores e sistemas tem crescido de forma vertical, e se prevê um crescimento contínuo em todo o mundo, e a pirataria de sistemas e programas tem ameaçado seriamente o futuro econômico desta industria. A cópia ilegal de programas obstaculiza a inovação e destrói os incentivos econômicos necessários para a criação de novos programas e aplicações.

Em razão disso é que se deve aplicar com rigor as normas existentes a coibir tias práticas delituosas, bem como, incentivar a edição de legislação que possa acompanhar a evolução dos programas e das técnicas de vilipendio dos direitos

intelectuais.

CRIMES DE INFORMÁTICA EM ESPÉCIE

Contra um sistema de informática

Os atentados contra o sistema de informática podem, de acordo com o objeto material da ação apresentar duas modalidades, as ações dirigidas contra o próprio computador, enquanto elemento físico, suas peças, acessórios, ou contra dados e informações nele contidos.

Contra o computador

Aí estão compreendidos os furtos comuns do próprio computador, do material de que é feito ou seus componentes, a sua apropriação indébita, portanto, até aqui, plenamente tipificados e resolvidos no âmbito da legislação comum. Não merecendo, todavia, a comporem os *crimes de informática*, pois o computador representa apenas um objeto, como outro qualquer, sobre o qual recaí a ação criminosa, de modo que se trata de crime contra o patrimônio. Portanto, delito comum.

Quando a ação criminosa visa a ser a danificação, sabotagem informática, inclusive os atos praticados contra os suportes materiais da informação, como disquetes, fitas magnéticas, etc., são, essencialmente, delitos que devem ser classificados como *crimes de informática*, pelas suas características e objetivo do autor dessa conduta ilegal .

Torna-se, de outra banda, muito mais difícil quando envolve situação em que é necessária a interpretação, no campo prático, dos chamados furtos de uso do computador, ou furto de tempo do computador. Tal utilização abusiva do computador consiste no uso desautorizado pelo proprietário, geralmente cometido por empregado, durante ou fora de suas horas de trabalho, com o fim específico de auferir proveito próprio.

A ocorrência costuma ser enfrentada com indulgência pelos lesados, todavia, seja reprimida em algumas legislações pois não deixa de representar um desfalque patrimonial ou desapossamento da coisa por certo lapso de tempo, além de importar no desgaste do material e da máquina, quando não a sua perda.

No Brasil, sabidamente não é prevista na norma material penal, porém existem criações jurisprudências, que, via de regra, têm descaracterizado a conduta do furto de uso, pois os julgados são rigorosos no sentido de que para ser caracterizado o furto de uso exigem enérgicas condutas, quais sejam, o uso momentâneo da coisa subtraída e sua devolução intacta no lugar de onde foi retirada; ausência de ânimo de apropriar-se da coisa. E, assim é manifesta a Jurisprudência:

"Para a caracterização do furto de uso a coisa subtraída depois de usada normalmente, deve ser imediatamente devolvida . Não basta a simples intenção de devolvê-la nem a alegação de que circunstâncias independentes da vontade do agente impediram-no de restituí-la. A prevalência da ilicitude da ação é sempre dirigida em relação ao fato genérico, isto é, o furto comum"(TACRIM-SP AC - Rel. Renato Mascarenhas - JUTACRIM 80/402).

Demonstra-se, portanto, que atendidos requisitos elencados, sempre o julgador atenderá ao acusado, que é absolvido quando a coisa foi subtraída sem ânimo definitivo de apropriar-se e depois devolvida, num curto espaço de tempo, nas mesmas condições e estado que estava anteriormente. Nos casos dos veículos assim furtados, os Tribunais exigem, porém, que a gasolina gasta seja recolocada pelo usuário antes da devolução, sob pena de ficar caracterizado o furto do combustível, esse sim merecedor de sanção.

Nessa esteira, seguramente, os nossos Tribunais chamados a manifestar-se sobre o furto de uso num caso concreto, é muito provável apliquem os critérios para isentar de punição o seu autor, principalmente se a ação se restringir à subtração de tempo e disponibilidade da máquina simplesmente.

Contudo, tal entendimento é aceitável para casos em que o prejuízo é irrelevante, porém, não será solução satisfatória para atender a situações em que o prejuízo seja de monta, ou se tal conduta é freqüente, ou, ainda, fique caracterizado um abuso de confiança , também não incriminado na nossa legislação.

Exsurge, desta conduta de *"furtum usus"*, a possibilidade de furto de energia , como já decidiu a Corte de Cassação belga, em 23.09.81, já que a lei penal brasileira, em matéria de furto, equipara à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Embora tais soluções, furto da energia elétrica ou de arquivos ou relatórios formatados, também, parece-nos inadequado, pois, não se trata de penalizar a ínfima consumação feita pelo autor, ou o desgaste irrisório do computador,

mas sim o enriquecimento ilícito em detrimento do proprietário do computador.

Seria necessário, haja vista que não existe no nosso Código Penal a figura de furto de uso, que se cuidasse dessa situação na legislação especial, na área especifica de informática. No presente resta tão somente ao proprietário do computador buscar a via judicial civil para ter ressarcido o seu dano e/ou prejuízo.

A prática delituosa conhecida no meio informático como "superzapping", que é a quebra do programa do computador. É a paralisação do computador, impedindo que ele realize operações normais e, com isso, permite o acesso ao banco de dados e memória e, portanto, a todo o sistema informático.

Contra dados e/ou sistemas de computador

Atos contra as informações que o computador mantém e fornece podem consistir na cópia desautorizada das informações nele contidas, na alteração de parte ou o todo das informações armazenadas pelo computador, ou a destruição completa dos dados pela exclusão do conteúdo dos suportes.

a) a cópia desautorizada, também chamada de *pirataria informática*, não se enquadra na apropriação indébita nem no delito de furto, pois não se trata de coisa corpórea, mas de informação copiada. Nem há subtração pois seu proprietário não é desapossado dela. Não havendo também estelionato, pela ausência de meio fraudulento, a questão deve ser remetida para a área de proteção da propriedade imaterial, ou, mais precisamente aos direito do autor, embora, ao nosso entendimento se trate de delito de informática, como já externado em sua amplitude e definição.

b) outra forma de atentados contra os dados e/ou informações, a alteração dos programas do computador que pode ser efetuada pela troca de cartões, discos ou fitas por outros de conteúdo falsificado ou modificados permitido o acesso a banco de dados, registros e codificações, também classificado espionagem de informática.

Tal fato também é tratado no âmbito do direito autoral e a exclusividade da utilização dos programas, porém, pode e invariavelmente envolve procedimentos de falsificação, portanto, passível de ser incriminada na legislação penal comum.

Uma das mais conhecidas técnicas consiste na sabotagem de um programa, a qual consiste em se colocar no computador outras instruções no lugar das originais, ou outro programa que irá coexistir com o original, alterando-o sem destruí-lo.

Esses fatos deveriam ter pelo legislador um cuidado maior, atentando a uma tipificação mais completa, pois a legislação que trata do direito do autor não seria suficiente para atender, porque comporta outros bens ou interesses que deveriam ter a proteção jurídica.

c) ainda poderia ocorrer a destruição total do programa do computador, seja pela exclusão (apagamento) do conteúdo dos suportes, seja pelo desvio de comando, com graves danos ao usuário.

Inserem-se nesta categoria os diversos métodos de atentados que são conhecidos por contaminação ou introdução de vírus no computador, que invadem os equipamentos destruindo ou alterando programas ou, ainda, impedindo o acesso a eles.

É um fenômeno recente e temido, o vírus eletrônico, que nada mais é do que a introdução de um programa no computador, que se reproduz sem autorização do usuário e interfere nos procedimentos normais da máquina, após ser ativado pelo próprio funcionamento do computador.

No Brasil são inumeráveis os computadores de empresas que tiveram elevados prejuízos pela inoculação desses programas que são chamados de vírus do computador, inclusive, empresas de grande porte como Petrobrás, Embratel, Banco Real, American Express, White Martins, BNDES, Universidade de São Paulo, PUC-RJ, e, o mais recente os computadores do Hipódromo da Gávea, no Rio de Janeiro, por ocasião do último Grande Prêmio Brasil, que foram inoculados pelo vírus Hiroshima 50 anos, que causou prejuízos elevados.

Os vírus chegaram ao Brasil pelas cópias piratas, outros são criações brasileiras, porém, são competentes para alcançarem seus objetivos, quase sempre devastadores. Uns são até benignos, como o *"ping-pong"*, não causam danos aos computadores ou seus arquivos, contaminam apenas os disquetes do usuário. Outros, porém são devastadores, como o *"sexta-feira 13"*, torna o computador mais lento, além de apagar os arquivos, e o tradicionalmente mais terrível, o *"madona"* que ao final de um *strip-tease* da cantora, avisa que o disco está se apagando.

De acordo com a Universidade Federal de São Paulo, os computadores podem ser contaminados por três modos diferentes:

- **quando um disquete com vírus é introduzido no computador;**

- **quando programas e dados são passados por linhas telefônicas, através de modem de transmissão e**

- **através de teclado, quando uma pessoa abre um programa e introduz, intencionalmente, um vírus.**

Também a técnica denominada *"lata do lixo"* que consiste na procura em latas de lixo, especialmente dos grandes edifícios de escritórios, onde estão as matrizes dos grandes conglomerados, de restos de lançamentos de computadores, ordens, códigos, linguagem e outras informações.

Deve ser incluído o denominado *"vandalismo"*, que consiste na destruição quer da máquina quer dos sistemas de processamento. Esses ataques são normalmente armados e são usados, na destruição dos equipamentos, bombas. Fatos desse gênero ocorreram na Austrália, África do Sul e Alemanha.

Ainda que se possa atribuir a empregados descontentes com a empresa, o mais comum é de terceiros ligados a ex-empregados. Outro tipo de vandalismo, mais civilizado, porém, ao sistema, altamente letal, é a destruição dos meios de armazenamento, seja pela destruição física ou por desmagnetização. Este, considerado o meio mais *"asséptico"*.

Assim, por clara, a facilidade e o perigo que representam essas ações quando intencionalmente efetuadas por alguém para causar danos ao empregador ou concorrentes.

O enquadramento típico como dano intencional muitas vezes não reflete a amplitude do problema e da situação, pois essa conduta delituosa só se verifica na hipótese da ocorrência de prejuízos patrimoniais.

Um dos meios que os usuários encontraram para protegerem-se dessas investidas criminosas foram os programas de diagnósticos desenvolvidos para identificar e detectar a presença de certos vírus, além de informar procedimentos a serem seguidos pelo usuário em face de uma contaminação.

De outra, medidas preventivas podem ser tomadas e têm sido amplamente divulgadas, de modo a neutralizar os resultados danosos dessas ações, e, em casos extremos devém ser punidas com sanções previstas na lei civil e na lei penal.

Por intermédio de um sistema

Contra o patrimônio

Destaca-se o furto, o dano e o estelionato como as formas mais usuais de infrações contra o patrimônio, vez que, praticamente todas as infrações podem ser cometidas pela utilização de sistema de informática.

O estelionato, que é caracterizado pelo emprego de meios fraudulentos para obtenção de vantagem ilícita, alcança os exemplos mais conhecidos e mais freqüentes dessas condutas criminosas.

Destaca-se o caso de desvio, em geral praticada por funcionário, de frações de quantias ou contas arredondadas nos cálculos financeiros de clientes ou de empresas, acumulando-se lentamente em conta pessoal determinado pelo delinqüente.

De outra forma, através do uso de cartão personalizado, fornecido por instituições bancárias, para funcionar nas contas eletrônicas, por meio de código pessoal, de que o agente delituoso se apoderou por meio de furto, falsificação, ou mesmo tendo encontrado o cartão.

Neste caso, quando o próprio usuário do cartão utiliza para sacar valores além do limite, complica-se e carreia uma gama imensurável de entendimentos doutrinários em torno da questão. Entre nós, ampla a conceituação legal do estelionato permite compreender nessa figura qualquer vantagem ilícita em prejuízo alheio, por qualquer meio fraudulento, e facilita a sua aplicação.

Contra a liberdade individual

Nessa, a informática é meio para violar direitos à intimidade, ao segredo ou à liberdade das comunicações.

A fraude informática presta-se, com perfeição, à revelação de segredos. Dependendo do caso, a ação poderá ser tipificada por violação de correspondência, violação de segredo ou violação de segredo profissional, todas perfeitamente tipificadas no Código Penal , como crimes contra a liberdade individual.

É garantido a todos o direito de à intimidade e à vida privada, bem como à imagem da pessoa pela Constituição Federal de 1988, no seu artigo 5º, inciso X, o qual garante o direito à indenização pelo dano material ou moral decorrente de sua violação. Porém, a lei penal vigente não prevê adequada proteção a esses interesses, que são alvos constantes pela utilização de novas técnicas eletrônicas ou sistemas de informática.

Contra a propriedade imaterial

Presta-se com eficiência a informática para a prática de violações dos direitos da propriedade literária e artística e, também, dos privilégios de invenção. Esses ataques são regulados pela legislação sobre direito autoral, na qual são definidas as modalidades, indicando sanções, que, por enquanto, face a inexistência de legislação específica, podem ser aplicados a determinadas condutas que se utilizam do computador e dos seus sistemas.

Na mesma medida e com o mesmo entendimento, as condutas que violam os privilégios de invenção, regulam-se pelo Código de Propriedade Industrial, e, na ausência de legislação específica aos delitos cometidos por meio de sistema de computador.

Via INTERNET

É importante que se tenha claro que a cada nova criação ou avanço tecnológico na área de informática também avançam os *crimes de informática* ou pela informática. Principalmente, quando exemplificamos, neste trabalho, que o computador e os sistemas que nele operam poderiam ser instrumentos de delitos comuns, não exageramos, pois no exemplo dado que, se através de um computador, pudesse ser dado uma ordem para matar alguém, por meio de várias combinações, seria um delito comum de informática. Para tanto, reproduzimos duas matérias publicadas em O Globo (1995, p.51), que dão a exata dimensão do uso do computador nos crimes comuns e do que o avanço tecnológico trouxe o uso delituoso da informática:

"JOVENS SÃO ATRAÍDOS POR INTERNAUTAS EXPERIENTES

Washington - A maioria dos menores nas casos já apurados de CIBERSEX foi atraída por adultos que se passavam por jovens, no computador. Um deles Alan Barlow, funcionário do Correio em Seatle, foi condenado a seis anos de prisão por ter tido relações sexuais com uma menina de dez, e também por ter tido contados obscenos por via eletrônica com meninos de vários estados. Uma lei federal, já em vigor, diz que é crime atrair menores a relações sexuais. Além disso, transportar material pornográfico de um estado para outro também é crime. Por isso, vários juristas têm opinado que não seria necessária mais uma lei para coibir abusos. O caso de Barlow, um inveterado usuário das BBS pornográficas encontradas na INTERNET ilustra isso. Ele acabou caindo numa armadilha banal: foi preso em Mamaronack, no estado de Nova York, onde tinha marcado, por computador, um encontro com um adolescente de 14 anos, com quem vinha se correspondendo obscenamente via "e-mail". Nestas intensas conversas por escrito, ele dizia ter 13 anos. Na verdade tem 51."

"SEXO "ON-LINE" NOS EUA SEDUZ ADOLESCENTES E DESAFIA A CENSURA (Jose Meirelles Passos- Correspondente)

Washington - Depois de dois dias de desespero, sem qualquer pista ou informação correta da Polícia sobre o paradeiro de sua filha Tara, de 13 anos, Lisa Noble decidiu ligar o computador da menina e verificar o seu "e-mail" - Correio Eletrônico. "Venha para cá. Nós poderemos correr pelo quarto, nus, o dia todo, a noite toda", dizia a última mensagem enviada à menina de St. Mathews, subúrbio de Lousville, em Kentucky. O convite era assinado por George e vinha de longe, de São Francisco, Califórnia. Logo depois, revirando sua gaveta, ela encontrou cópias impressas de diálogos que Tara vinha mantendo com George durante várias semanas. O material era típico CYBERSEX, isto é, sexo cibernético, como vêm sendo denominadas as conversas sexuais via computador, a cada dia mais abundantes e intensas, e que agora estão sob ameaça de censura pelo Governo do EUA. Dias atrás, cinco casos semelhantes ao de Tara Noble serviram de argumento no Senado para aprovar a chamada Lei de Decência das Comunicações por ampla maioria de votos (84 a 16), provocando uma polêmica nacional. Muita gente crê que ela infringe o direito de livre expressão, sacramentado na Primeira Emenda da Constituição americana. Todos os cinco casos registrados desde janeiro passado envolveram crianças e adolescentes - descritos como CYBERPORN, a pornografia cibernética que circula através da INTERNET, o sistema interliga hoje 50 mil redes com cerca de 35 milhões de usuários (também conhecidos por internautas), em pelo menos 150 países. "A INTERNET tem sido chamada de enorme e ilimitada biblioteca internacional. E a emenda Exon limita a todos nós à seção infantil dessa biblioteca", reagiu Mike Godwin, advogado da Eletronic Frontier Foudation, instituição que promove informática. Um dos problemas da lei será a execução. Em muitos casos é impossível descobrir o autor de uma mensagem eletrônica. Quando a mãe de Tara Noble revelou o seu achado à Polícia de Lousville, o delegado local entrou em contato com o FBI - a Polícia Federal americana - e também com o Serviço Secreto. Agentes de suas respectivas Unidades de Crimes por Computador foram mobilizados. Mas a menina só foi encontrada porque ela mesma acabou ligando para a mãe, 13 dias depois de seu desaparecimento. "Mamãe quero voltar para casa", disse ela, de um telefone público, revelando seu endereço em São Francisco. No dia seguinte enquanto a mãe a levava de volta, o FBI prendia George por ter tido relações sexuais com uma menor.

Descortina-se, pelos artigos reproduzidos, que a rigor não são *crimes de informática*, ao nosso entender, porém, a informática foi instrumento de preparação de um delito comum, qual seja, entre nós, crimes contra a liberdade sexual.

Afloram, de tais fatos, em nosso ordenamento jurídico, crimes de estupro qualificado (arts. 213 e 224, do CP) e posse sexual mediante fraude (art. 215, do CP), demonstrando que a informática pode ser instrumento hábil para serem alcançados delitos comuns, e, nem por isso ser classificado como *crime de informática*.

Ainda, observa-se da matéria reproduzida que a norma aprovada pelo Senado Americano - a Lei de Decência da Comunicações - insere a conduta delitiva na correspondência via INTERNET. Desde já, e sem a profundidade de se conhecer o texto exato da norma, se transplantada para o Direito Penal pátrio, exsurgem dificuldades, tais como qual o foro competente ? O Código Penal

adota a teoria finalista da ação, onde foi consumado o delito? Pode admitir a forma tentada ou a possibilidade de dolo ou culpa? Pode ocorrer o concurso de normas e de delitos?

Assim, ao nosso entender, esse tipo de crimes especiais, que envolvem crimes comuns e *crimes de informática*, devem ser avaliados pelo legislador brasileiro, pois as redes, a INTERNET é uma realidade em nossas casas, hoje, e, prestam-se a muitos outros tipos de delitos que estão inseridos ou não no Código Penal e na Legislação Penal Extravagante. Todavia, toda e qualquer legislação sobre *crimes de informática*, se forem meios a outros, não podem seguir a regra subsunção aos delitos comuns, pois assim, não evoluímos no Direito Penal de Informática, porque os operadores do direito têm que experimentar um regramento nesse sentido, para construírem esse Direito que não é futuro, é presente.

O Direito penal de informática vigente

O Direito Penal de Informática caracteriza-se pela sua absoluta pobreza. A Parte Especial do Código Penal data de 1940 e as normas incriminadoras são de um tempo em que sequer existia o computador, de modo que as normas vigentes somente podem ser aplicadas aos *crimes de informática* de forma incidental a tais hipóteses.

O legislador brasileiro somente preocupou-se com o mau uso do computador, vez que a legislação existente dirige-se especificamente à pirataria de *"software"*, jamais ao *crime de informática*, por excelência.

Também, os doutrinadores brasileiros acompanham a tendência internacional que protege o *"software"* ao entendimento do que seja direito autoral. O legislador aceita essa posição. Para tanto, a Lei 7.646, de 18 de dezembro de 1987, definiu em seus artigos 35 e 37 dois crimes que expressam esse entendimento:

Art. 35 - Violar direitos de autor de programas de computador:

Pena: Detenção, 6 (seis) meses a 2 (dois) anos e multa.

Art. 37 - Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:

Pena: Detenção, de 1 (um) ano a 4 (quatro) anos e multa.

O artigo 35 retrata, com clareza meridiana, o objetivo do legislador em proteger o direito autoral, sem, contudo, mesmo assim, ser caracterizado como um *crime de informática*, e, sim, crime contra o direito autoral.

O artigo 37 cria a figura típica de contrabando de informática. O objeto jurídico é, tão somente, o erário público, prejudicado pela evasão da renda e da proteção dos "*softwares*" nacionais. Também, a norma carrega a amplitude da incidência genérica, tal como, no artigo 334 do Código Penal, o delito de contrabando e descaminho.

Pela simples leitura, vê-se que as regras legais citadas são manifestamente imperfeitas e insuficientes para os fins que se destinam, tanto assim, que com a mudança em matéria de política de informática, o delito de contrabando de *"software"* não cadastrado, já não mais tem razão de existir, vez que, hoje, não mais é necessário que seja cadastrado junto ao Ministério da Indústria e Comércio.

Ainda, ao apreço da norma nacional, que tem por finalidade, apenas, proteger a propriedade intelectual, em relação ao programa de computador, como manifestação de propriedade imaterial, fazendo-o da mesma forma que o Código Penal o faz, para a violação do direito autoral em geral. Todavia, a pena prevista é, em muito mais gravosa que a determinada pela Lei Substancial Penal (detenção de três meses a um ano e multa).

O sistema legal ainda contempla proteção aos crimes contra a ordem econômica e contra as relações de consumo. No âmbito da ordem tributária, a Lei n. 8.137. de 27 de dezembro de 1990, define uma nova forma de mau uso do computador, qual seja, ação de utilizar ou divulgar programa de processamento de dados que permita ao contribuinte possuir informação contábil diversa que é , por lei, fornecida à Fazenda Pública, sendo apenado com detenção de seis meses a dois anos e multa. É, pois, um programa de computador destinado a permitir a fraude fiscal.

Ante essa paupérrima legislação, o aplicador do direito é obrigado a servir-se dos delitos tradicionais para o combate aos *crimes de informática*. Têm-se que muitas das condutas que caracterizam o *crimes de informática*, poderiam ser enquadradas na figura típica do estelionato. Todavia a velocidade do desenvolvimento tecnológico no setor de informática, não garante que se possa, eternamente, manter a aplicação do nosso Código Penal, ou seja, o enquadramento dos crimes comuns às condutas típicas do delitos de informática. Some-se a essa dificuldade presente, as diversas doutrinas e

correntes que pululam a matéria criminal de informática, e mais, as próprias divergências em torno da aplicação do Direito Alternativo e a corrente que defende programa de descriminalização, que vertem profundas dificuldades ao aplicador do direito.

O projeto da nova Parte Especial do Código Penal

A proposta da nova Parte Especial do Código Penal, que deverá ser apresentada pelo Ministério da Justiça ao Congresso Nacional, no que diz respeito à tutela penal dos interesses e dos bens advindos ou redefinidos em sua importância, pela Sociedade de Informação Pós-Industrial, caracteriza-se por estabelecer um caminho próprio.

Os *crimes de informática* estão contidos em um Capítulo do Código Penal definidos como "Dos Crimes Contra à Ordem Sócio-econômica", da Parte Especial do Código Penal. O supracitado Capítulo conta com apenas oito artigos. Três destes artigos tratarão, especificamente, dos *crimes de informática*, enquanto outros três dispositivos tratarão da adequação de normas já existentes aos bens intangíveis redefinidos na 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.

LICKS e ARAÚJO JÚNIOR (1994, p. 98), assim analisam essas novas normas, afirmando que *"podemos dizer que, enquanto três artigos tratarão de computer crime, outros cinco estarão relacionados com o computer misuse."*

Vê-se, pois, que os doutrinadores, a priori de um entendimento crítico, tanto no aspecto quantitativo, bem como o qualitativo, porque o Direito Da Informática, "in casu", o Direito Criminal da Informática, face a tantas doutrinas e as próprias complexidades apresentados pela Ciência da Informática, seguramente, não poderia o Brasil, tratar essa área do direito, não mais emergente, todavia, cada vez mais presente na vida do povo brasileiro, com tão pouca profundidade.

Propostas

Nessa nau de incerteza quanto ao Direito Criminal de Informática, e, também pode-se dizer, da própria incerteza do Direito Criminal Brasileiro, verifica se que outros projetos tramitam no legislativo brasileiro. Atualmente, estão em

tramitação no Congresso Nacional os seguintes Projetos:

- 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. E, foi absorvido por outro, de n. 137 de 1989, que assim é redigido:

Art. 1º - - 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.

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

Pena - detenção de três meses a um ano.

Art. 2º - 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. 3º - A Ação Penal, nos crimes previstos nesta lei depende de representação.

O projeto não é, especificamente, uma norma voltada aos *crimes de informática*. É, na verdade, uma miscelânea entre o direito de imagem, a privacidade, e mau uso do computador. Além disso, pela sua vinculação aos delitos contra a vida privada e imagem, dependem de representação, enquanto que os *crimes de informática* não devem ser inscritos pela dependência de representação, e, sim, nos delitos de ordem pública.

- Tramita na Câmara do Deputados o Projeto n. 4.597, de 1990, que foi substituído pelo de n. 597, de 1991, que dispõe sobre o crime de interferência nos sistemas de informática, com a seguinte redação:

Art. 1º - Pratica crime quem, objetivando prejuízo de alguém, a um sistema, a computador, a equipamento que acompanha o sistema ou a computador:

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

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 de igual ao valor do proveito visado ou do risco de prejuízo da vítima;

c)introduza, dolosamente, em computador, computador ou instrução-comando que destrua ou altere programa armazenado no computador, ou por qualquer forma que 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 ao igual valor do proveito visado ou do risco de prejuízo da vítima;

Art. 2º - A interferência não intencional, por negligência, impudência 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.

O projeto supra tem características mais próximas do que almejam os doutrinadores brasileiros, embora, ainda esteja distante, não da perfeição jurídica, do mínimo que atenda ao presente tecnológico, de modo a proteger o sistema, o computador, seus periféricos, e também o uso adequado.

Apesar de não preencher às necessidades da área de informática, é o mais completo, e tem nos especialistas, tanto da informática como do direito, ferrenhos defensores da sua aprovação. Todavia, entendemos que a normatização dos *crimes de informática* devem ser mais amplos, abrangendo um maior leque de condutas, bem como, ao detalhamento, pois vê-se que o projeto utiliza-se de verbos nucleares de grande abrangência, permitindo a criminalização de condutas que não são, ao nosso entender, passíveis de mensurá-las, tais como abuso, pois o conceito de abuso é amplamente subjetivo, o que permitiria inadequação da norma penal no mundo dos fatos.

O Sr. Presidente da República remeteu mensagem ao Congresso Nacional, de modo a dar seqüência à política de liberação dos meios de informática. Essa mensagem foi transformada em Projeto de Lei n. 997/91, que regula a proteção da propriedade intelectual de programas de computador e sua comercialização no País, e , dele exsurge:

- **eliminação das restrições a empresa nacional para distribuição e comercialização de programas de computador de origem externa;**

- **a eliminação do exame de similaridade entre o produto estrangeiro e o nacional;**

- **eliminação do cadastramento de programas de computador;**

- **possibilidade de importação de cópias de programas de computador sem contrato de distribuição, objetivando maior competitividade do setor;**

- **reforços aos direitos e garantias aos usuários de programas de computador.**

O Projeto de Lei de autoria do então Senador Maurício Corrêa, que leva o n. 152, de 1991, a muitos tem a característica de ser o que introduz as maiores e mais importantes inovações, pois visa a garantir os dados de propriedade do usuário, de modo que o bem a ser protegido é a inviolabilidade dos dados e da comunicação. Entende, ainda, o projeto, que não se criaram novos crimes, o que foi alterado é a forma de cometimento dos delitos.

Assim, pois é o texto do projeto:

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

Art. 2º - 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 e multa.

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

Pena - detenção de três meses a um ano e multa.

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

Art. 3º - 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.

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

Pena -detenção de seis meses a dois anos e multa.

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

Pena - Detenção de um a três anos e multa.

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

Art. 5º - 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 e ideológica nos termos do Código Penal, como qualificadora do art. 4º desta lei.

Parágrafo Único - Para fins deste artigo considera-se "documento público" a informação 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."

Vê-se, pois, que o projeto é abrangente, inovador, porém, ainda, observa-se que a generalidade é a tônica dos verbos nucleares do tipo. É, ratificamos, necessário que as condutas sejam pormenorizadas, de modo a dar a característica do tipo que se quer punir. Apesar dos avanços, em termos de projeto, já que a legislação brasileira é pobre sobre o tema, é importante que os *crimes de informática* sejam normatizados ao abrigo do conhecimento técnico de condutas ilícitas, evitando-se, assim, as lacunas ocasionadas pela generalidade do seus núcleos.

CRIMES DE INFORMÁTICA (V)

De Lege Ferenda

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)

Em princípio tínhamos a pretensão de, ao final deste trabalho, sugerir um conjunto de normas que, no nosso prisma, viriam a preencher as lacunas da Lei Penal vigente.

Todavia, ao compulsarmos o brilhante trabalho de LICKS e ARAÚJO JÚNIOR, (1994, p. 101-103), deparamo-nos com sugestivo conjunto de normas por ele propostas, que seriam incluídas em nosso Códex Material Penal.

As normas propostas têm o condão de quase exaurir, no nosso entendimento, os mais variados delitos de informática. Em razão disso é que deixamos de propor normas nesse sentido, as quais não teriam a felicidade de LICKS e ARAÚJO JÚNIOR, além do que poderiam ocasionar a sobreposição de normas, na sua forma *"de lege ferenda"*.

No entanto, nos permitimos a transcrevê-las acrescidas com nossa limitada exegese, bem como, nos permitimos, quando necessário, desposar crítica em torno da sua aplicabilidade aos delitos de informática.

Por outra, ao longo da nossa comunhão com as normas propostas, procuramos manter claro o que é da lavra dos seus proponentes e o que seja da nossa autoria, assim preservando e respeitando aos autores.

Também é de ser aclarado que as observações são sucintas, pois, se aprofundadas desvirtuarse-iam os objetivos desta obra.

PROPOSTAS DA NOVA PARTE ESPECIAL DO CÓDIGO PENAL
Dos crimes contra sistemas de processamento ou comunicação de dados

Violação de sistema de processamento ou comunicação de dados

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

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

Objeto jurídico

Visa a tutelar o acesso indevido aos dados e sistemas contidos em um conjunto informático (*"hardware"* e *"software"*). Inova quando atribui à tentativa a mesma pena. Tal entendimento vem do conhecimento dos meios informáticos, vez que, por exemplo, a simples ação de ligar o equipamento, o agente já estará produzindo funções no sistema, qual seja, o da auto-configuração do *"hardware"*, independentemente de uso de senha. Portanto, demonstrando o conhecimento técnico de informática, a proposta acerta na sua extensão tipificadora.

Por mais inovador, ainda, é que, no âmago da norma, é apenado o furto de uso, jamais criminalizado no Direito Penal brasileiro.

Sujeitos ativo e passivo

Sujeito ativo é toda pessoa física que viola o conjunto informático, produzindo qualquer função. O sujeito passivo pode ser qualquer pessoa física ou jurídica, que tenha a posse ou a propriedade do conjunto de informática.

Ação física

É todo ato em que o agente acessa ou tenta acessar um conjunto informático alheio sem autorização, portanto indevidamente.

Elemento subjetivo

O dolo é genérico. Do texto da norma não se depreende exigir específico. Aquele é a vontade consciente em acessar indevidamente conjunto informático alheio. A culpa é admissível, porém, com restrições e muito bem caracterizados os atos exteriores do agente.

Consumação e tentativa

Vêm expressas no próprio tipo; contudo, inova ao incluir na mesma pena, sem qualquer redução, a tentativa.

Pena

Aplicam-se ao tipo as penas de multa e impedimento de atividades ligadas à informática. Trata-se de inovação em nossa legislação penal, e carreia entendimento do direito norte-americano em relação aos crimes ligados à profissão. Reitera-se a apenação na mesma intensidade ao delito na sua forma tentada.

"Formas Qualificadas"

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

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

Nesta qualificadora, buscam os proponentes punir aquele agente que, indevidamente, pratica atos que causem danos ou deles obtenha vantagens. Aqui a proposta é, pois, de punir o vândalo da informática e o delinqüente que se utiliza do computador de outrem. A pena, no nosso sentir, deve ser acrescida de um terço até a metade.

"§ 2º. 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."

Qualifica a conduta do agente que, ao acessar indevidamente o conjunto informático, causa alteração temporária ou permanente, protegendo a integridade do *"hardware"* e *"software"*. Vislumbra-se a primeira norma em que é tipificável a inoculação dos denominados *vírus do computador*.

"§ 3º. 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 e interdição para o exercício de atividade ligada à informática por ... anos."

Qualifica o meio fraudulento da aquisição do acesso indevido. Entendemos que nesta norma se deveria punir ao detentor autorizado de senha ou meio de acesso, que cede a outrem desautorizado.

"§ 4º. Se, com o acesso indevido, o agente devassa sigilo de dado 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."

Qualifica o acesso indevido, como também amplia o conceito de violação de segredo (art. 153/154, do Código Penal), pela especialização da ferramenta utilizada.

"§ 5º. 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."

Qualifica a conduta do agente que ao acessar causa dano ou obtém vantagem, embora a norma dê a entender que o agente não buscava o resultado dano ou vantagem. Desse modo, nos parecer ser conduta culposa e não dolosa em relação aos efeitos do acesso indevido.

Atentado contra a integridade de sistema de processamento ou comunicação de dados

"Art. 2º. Desenvolver comando, instrução ou programa 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."

Objeto jurídico

Trata-se de norma multinuclear que visa a proteger a incolumidade do equipamento de informática. É norma que ao nosso entender deveria ser desdobrada em tipos específicos, de modo a atender, minuciosamente, as condutas delitivas.

Sujeito ativo e passivo

Sujeito ativo é qualquer pessoa física que se utiliza dos meios informáticos a produzir dano ao sistema e/ou vantagem com o dano produzido. O sujeito passivo é qualquer pessoa física ou jurídica que tenha a posse ou a propriedade do sistema de informática.

Ação física

É o conjunto de atos que caracterizam o uso dos meios informáticos, por qualquer via, direta ou por comunicação, que produzam dano, vantagem ou ainda pela simples realização pessoal de produzir os resultados do tipo apenado.

Elemento subjetivo

É o dolo genérico. A clandestinidade exposta no tipo extirpa a possibilidade da forma culposa, embora seja admissível, porém muito difícil de ser caracterizada, pois basta a ação ser clandestina para configurar a vontade do agente.

Consumação e tentativa

Não basta o agente desenvolver comando, instrução ou programa de computador, estes devem ser capazes, clandestinamente, de produzirem diversas ações. É necessário que estes produzam os resultados danosos ao equipamento para se ter o delito consumado. Se percorrido o tipo e não alcançado o resultado, clara é a forma tentada.

Pena

Entendemos que a pena alocada é branda em razão direita do objetivo material do agente, qual seja, o equipamento, pois visa a produzir ações com o fim de danificá-lo, de obter vantagem ou por mera satisfação pessoal. Trata-se de delito que agride o patrimônio, e em nosso Código Penal o legislador sempre apenou de forma contundente os crimes contra o patrimônio, que aqui deveria ser agravado em função da alta especialização do agente. Por mais, é de ser lembrado que as condutas de inoculação de vírus, podem ser enquadradas, pois o objeto juridicamente protegido pela norma é o equipamento, e, se a ação típica do denominado vírus é obter os resultados elencados, é plenamente cabível a aplicação da norma.

"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."

O parágrafo único é a ampliação da proteção contra os agentes inoculadores de "vírus". Aqui o objeto protegido são os *"softwares"*, os principais alvos dos "vírus", embora estes também atinjam o *"hardware"*.

Sabotagem informática

"Art. 3º. Destruir, inutilizar ou deteriorar o funcionamento ou a capacidade de funcionamento de sistema 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."

Objeto jurídico

Tem como objeto material a ser protegido o conjunto informático. Se prismada a um ângulo restrito, poderia se afirmar que é uma sobreposição de normas. Entendemos que não, pois o objetivo é penalizar as condutas que têm o objetivo de causar dano de forma a prejudicar um procedimento produtivo.

Sujeito ativo e passivo

É toda pessoa física que produz as ações delitivas. Visualiza-se que o sujeito passivo em regra seja a pessoa jurídica, porém, perfeitamente aplicável à pessoa jurídica desde que tenha a posse ou propriedade do conjunto informático.

Ação física

É toda conduta que danifica o funcionamento ou reduz o funcionamento do *"hardware"* e/ou *"software"*.

Elemento subjetivo

É o dolo genérico. É a vontade livre e consciente de danificar ou reduzir a capacidade de funcionamento do conjunto informático. Inaplicável na forma de culpa, vez que o tipo exige que o agente objetive um resultado prévio.

Consumação e tentativa

A consumação do delito caracteriza-se quando alcançado o dano ou a redução da capacidade do conjunto informático. A tentativa é admissível.

Pena

Entendemos que a pena alocada é branda em razão direita do objetivo material do agente, qual seja, o equipamento, pois visualiza produzir ações com o fim de danificá-lo ou reduzir a sua capacidade. Trata-se de delito que agride o patrimônio, e em nosso Código Penal o legislador sempre apenou de forma contundente os crimes contra o patrimônio, que aqui deveria ser agravado em função alta especialização do agente.

Furto de tempo de rede de sistema de processamento de dados

"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."

Objeto jurídico

É a proteção aos sistemas de redes estatais, e as redes que prestem serviços públicos. Em nosso entendimento é a criminalização do furto de uso em que a vítima é o Estado.

Sujeito ativo e passivo

Ativo é qualquer pessoa física que se utilize de redes estatais, sem autorização. O sujeito passivo é sempre o Estado em suas mais variadas formas, já que amplia a abrangência para entidade governamental ou de caráter público, assim inserido, crê-

se, até as empresas de economia mista. É por demais abrangente, deve ser especificada a amplitude do agente passivo.

Ação física

Toda conduta que acessar, sem autorização, rede de processamento ou comunicação de dados das entidades estatais.

Elemento subjetivo

É a vontade livre e consciente de praticar furto de uso contra entidades estatais. Basta a ausência da autorização do uso, para que se consolide o dolo. De resto, não admite a forma culposa.

Consumação e tentativa

Consuma-se pelo efetivo acesso desautorizado às redes estatais. A tentativa, embora possa existir, pelos meios tecnológicos hoje disponíveis, inviável é a sua constatação.tentativa.

Pena

Atende a filosofia da norma proposta.

Tráfico de dados pessoais

"Art. 5º. Destinar dado ou informação de caráter pessoal, constante de sistema de processamento de dados ou em qualquer suporte físico, à 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."

Objeto jurídico

Visa proteger os dados pessoais do cidadão. É comum, por exemplo, recebermos em casa diversas correspondências de empresas com que jamais tivemos contato. Percebe-se que os nossos dados pessoais: nome, endereço, etc., foram fornecidos a essa empresa sem a nossa autorização. Há poucos anos atrás este exemplo era corporificado pelas revistas Veja e Isto É, que continham anúncio de vendas de cadastros. Estes cadastros eram coletados e comercializados de forma genérica ou

por setores, dependendo do interesse do adquirente.

Sujeito ativo e passivo

Sujeito ativo é todo aquele que detém informações de pessoas físicas e as repassa a outra sem autorização dos interessados. Sujeito passivo qualquer pessoa física. Embora devesse a norma abranger também as pessoas jurídicas.

Ação física

O simples fornecimento da informação a outrem, não autorizada.

Elemento subjetivo

É o dolo genérico. Inadmissível a culpa.

Consumação e tentativa

Consuma-se pelo fornecimento dos dados. Não admite a forma tentada.

Pena

Atende a filosofia da proposta.

Violação do dever de informar

"Art. 6º. Deixar de dar conhecimento ou retificar informação pessoal constante e acessável por sistema de processamento ou comunicação de dados ou 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."

Objeto jurídico

Visa à proteção do direito do cidadão em ter lançados nos registros oficiais as informações corretas. É comum, por exemplo, que os indiciados em inquéritos policiais tenham lançados seus dados pessoais em cadastro de antecedentes criminais, apesar de ser uma forma de violar garantias e direitos individuais prescritos na Carta Magna. Quando absolvido ou arquivado o inquérito não são apagados esses registros e, quando o cidadão necessita de atestado de antecedentes, tem a surpresa de ainda estar constando contra ele informações desabonatórias.

Deveria ser estendido às entidades não-governamentais, tais como cadastros de Serviço de Proteção ao Crédito SPC, e outros.

Sujeito ativo e passivo

Ativo é o agente público que deixa de fazer o lançamento de alteração ou inclusão de dados em cadastros necessários. Passivo é toda a pessoa física, embora entenda que deva ser, também, aplicável à pessoa jurídica.

Elemento subjetivo

É a vontade livre e consciente de não proceder o lançamento de registro de dados que o agente público tem de fazê-lo. Admite-se a forma culposa, expressa pela negligência.

Consumação e tentativa

Trata-se de delito que se consuma pela omissão de não proceder ao lançamento nos meios informáticos de dados pessoais da vítima. Inadmissível a tentativa.

Pena

A pena atende a filosofia da proposta. Como se trata de delito praticado por agente público, aplicável, em concurso, as penas do artigo 319 do Código Penal (prevaricação).

Equiparação a documento

"Art. 7º. 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.

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

Trata-se de norma de cunho processual, a qual inclui "*"software"*" e "*""hardware""*" como meios de provas. É um avanço no campo do Direito Processual Penal, porém, entendemos que deve ser melhor, mais profunda e tecnicamente detalhada, pois ao ser produzida como prova deve chegar ao processo de forma inteligível ao leigo em

informática, porque a sua forma originária, seguramente, causará divergências e dúvidas quanto ao seu aproveitamento pleno e como meio hábil de produzir efeitos no processo penal.

Crimes cometidos em outros capítulos

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

A proposta atende uma das preocupações que temos em relação aos *"crimes de informática"*. Entendemos que a informática é uma ferramenta poderosa para o cometimento de crimes, e, em nossa classificação já demonstramos essa preocupação.

CRIMES DE INFORMÁTICA (VI)

Conclusão e Bibliografia

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)

CONCLUSÃO

Ao concluirmos este trabalho constatamos que uma das muitas dificuldades que o tema propõe é a difícil interação dos *idiomas* utilizados, tanto pelo direito como pela informática, haja vista que o desconhecimento da terminologia leva o examinador a incorrer em equívocos na interpretação jurídica de condutas específicas e características da ciência informática.

O Direito Penal de Informática, como referencial científico, já é entre nós indelevelmente presente, inobstante que alguns assim não o reconheçam. Daqueles que o estudam, percebemos a nítida preocupação com a variedade e a velocidade com que se aprimoram os métodos delitivos, pois os números que orbitam a informática, a caba dia que passa, nos são apresentados em cifras elevadíssimas. Ao mesmo tempo em que cresce o uso de computadores, na mesma proporção multiplicam-se os métodos delitivos, que envolvem o conjunto informático.

Os conceitos compilados expõem a polêmica e a controvérsia, em razão da natureza e da complexidade do tema. Somando a essas, entendemos que estes delitos devem ser prismados à ótica do objeto material, do bem juridicamente protegido (ou a ser protegido). Em razão disto afirmamos serem os *crimes de informática***todos aqueles**

em que o agente se utiliza dos meios informáticos como instrumento ou fim do delito.

A partir deste conceito, possibilitou-nos que dividíssemos estes crimes em três categorias: *puros, mistos e comuns*.

Esta classificação permite que o legislador elabore normas próprias para coibir tais práticas delitivas, ao mesmo tempo em que pode aperfeiçoar as normas existentes e com isto abranger o universo deste tipo de crime.

Sugerimos que sejam incluídas qualificadoras pelo uso dos meios informáticos, às normas penais vigentes. Normas estas que atenderiam aos delitos mistos e comuns, restando ao legislador a criação de norma específica a atender aos delitos puros de informática.

Por outra, expusemos, embora que de forma sucinta, a aplicabilidade das normas penais existentes à algumas condutas, demonstrando, assim, ser possível a utilização das normas vigentes a estes delitos, embora saibamos serem deficientes para suportar os métodos criminais desta natureza. Também é de ser ressaltado que não ocorre o uso da lei penal vigente a estes delitos, pelo desconhecimento dos aplicadores do direito, o que tem remetido o delinqüente informático à impunidade. Credita-se, pois, tal afirmação, à complexidade e natureza dos delitos, que requerem dos aplicadores do direito sólidos conhecimentos de informática e de áreas afins.

De outra banda, pelos vários delitos descritos ao longo deste trabalho e, em especial aqueles que são perpetrados via INTERNET, nos foi dado perceber a profunda preocupação da comunidade penal de vários países com o crescimento de métodos sofisticados delitivos perpetrados através de infovias.

A exemplo da tratamento que foi dado ao cheque, é, pois, por oportuno que seja editada legislação unificada sobre crimes desta natureza, até porque o crescimento vertical da tecnologia de informática, por via de conseqüência, traz consigo, na mesma proporção, estes delitos. Também, é de ser alertado que com a oferta de infovias, se potencializam os delitos multinacionais, que por sua peculiaridade hoje oferecem profundas dificuldades no que concerne à competência para julgar tais delitos multinacionais.

Os métodos e exemplos de delitos que elencamos nos assevera que ao Brasil é muito importante que esteja preparado e na vanguarda deste tema para poder enfrentar com eficácia esses novos crimes..

Uma das constatações que aflora, embora que subsidiária ao tema deste trabalho, é que cresce de forma quase que incontida a corrida ao domínio da informática, pois o poder que emana do controle da ciência informática assemelha-se ao poder emanado pelos detentores da tecnologia nuclear em passado não muito distante. Também por estes motivos devem ser otimizados os procedimentos de pesquisa,

intercâmbio e aquisição de tecnologia, bem como, seja propiciado e incentivado o estudo jurídico do direito voltado à informática,

Calcados nestas razões e constatações, reiteramos que urge ao legislador pátrio dote os operadores do direito desta ferramenta, já imprescindível. Tais medidas visam a que o país tenha meios adequados para enfrentar esta nova realidade jurídica que é a informática e seus efeitos na vida do Estado e dos cidadãos.

BIBLIOGRAFIA

1 AMARAL, Sylvio do. Falsidade documental. 3. ed. São Paulo : RT, 1989. 213p.

2 ASCENÇÃO, J. Oliveira. Direito do utilizador de bens informáticos. Sequência, Florianópolis, v. 28, p. 55-71, jun 1994.

3 Aumentam os roubos de "chips". Zero Hora, Porto Alegre, 16 ago 1993. Zero Hora Informática, n. 106, p. 3

4 BLOOMBECKER, Buck. Crimes espetaculares de computação. Rio de Janeiro : LTC, 1992, 228p.

5 BUSSADA, Wilson. Falsidade documental interpretada pelos tribunais. São Paulo : Aquarela, 1988. 404p.

6 CERQUEIRA, Tarcísio Queiroz. Software direito autoral e contratos. Rio de Janeiro : ADCOAS, 1993. 371p.

7 CHALMERS, Leslie. Computer - assisted crime in backing: transit and delivery. In: Data Security Management. New York (EUA), n. 82, p. 12, june 1986.

8 CORREA, Antonio. Dos crimes contra ordem tributária. São Paulo : Saraiva, 1994. 285p.

9 COSTA, Cesar da. Crime computadorizado: as conseqüências não previstas no uso do computador. In: INTERFACE, São Paulo, v. 2, n. 16, p. 8-12, 1984.

10 COSTABILE, Henrique. Combatendo crimes por computação. BANAS. São Paulo, v. 25, n. 1182, p. 27-28, jul 1978.

11 DOTTI, René Ariel. Controle de informática. In: Revista dos Tribunais. São Paulo, n. 518, p. 265-266, dez 1978.

12 Estudantes copiaram programas ilegalmente. Polícia da Suíça prende dois piratas da Internet. Gazeta Mercantil. São Paulo, 20 jun 1995, p. 6.

13 FARIA, Bento de. Código penal brasileiro (comentado). Rio de Janeiro : Récord, 1959. v. III. 415p.

14 FERREIRA, Aurélio Buarque de Holanda. Novo dicionário da língua portuguesa. 2. ed. Rio de Janeiro : Nova Fase, 1986. 1838p.

15 FERREIRA, Ivete Senise. Os *crimes de informática*. In: BARRA, Rubens Prestes, ANDREUCCI, Ricardo Antunes. Estudos jurídicos em homenagem a Manoel Pedro Pimentel. São Paulo : RT, 1992. 9. p.139-162.

16 FRANCO, Alberto da Costa; STOCO, Rui; COLTRO, Mathias et al. Código penal e sua interpretação jurisprudencial. 5. ed. São Paulo : RT, 1995. 3358p.

17 FRANCO, Alberto da Costa; STOCO, Rui; COLTRO, Mathias et al. Leis penais especiais e sua interpretação jurisprudencial. São Paulo : RT, 1995. 1570p.

18 GARCIA, Basileu. Instituições de direito penal. 2. ed. São Paulo : Limonad, 1954. v. i. 395p.

19 GARDNER, Ella Paton; SAMUELS, Linda B.; RENDER, Barry. The important of ethical and legal standard in end-user computing. In: Data Security Management. New York (EUA), n. 82, p. 16. june 1986.

20 JEHORAM, Hermann Cohen. Proteção do "chip". In: Cadernos de Direito Econômico e Empresarial. Rio de Janeiro : RDP, jul/set 1991. p. 278-281

21 JESUS, Damásio E. de. Código penal anotado. 2. ed. São Paulo : Saraiva, 1991. 932p.

22 JESUS, Damásio E. de. Novas questões criminais. São Paulo : Saraiva, 1993. 177p.

23 Jovens são atraídas por internautas experientes. O Globo 9 jul 1995, p. 51.

24 Lei inglesa do uso indevido do computador de 1990, In: Revista de Informações Legislativas. v. 28, n. 111, jul/set 1991.

25 LICKS, Otto Banho: ARAÚJO JÚNIOR, João Marcelo. Aspectos penais dos *crimes de informática* no Brasil. In: Revista do Ministério Público, São Paulo : Nova Fase, 1994. p. 82-103.

26 LUCA, Jose Carlos Moreira de. A pirataria não compensa. Exame Informática. São Paulo, mai 1992. 8, n. 90, p. 118, set 1993.

27 MICHALOWISKI, Raynond J.; PFHUL, Erdwin H.. Technology, property and law. In: Crime, law and social change. San Francisco (EUA), v. 15, n. 3, p. 255-275, may 1991.

28 MIRABETE, Julio Fabbrini. Manual de direito penal. São Paulo : Atlas, 1991. v. I-III.

29 MONTEIRO, Samuel. Crimes fiscais e abuso de autoridade 2. ed. São Paulo : Hemus, 1994. 806p.

30 NEGROPONTE, Nicholas. O computador liberta. Veja, São Paulo, v. 28 n. 30, p. 7-10, jul 1993.

31 NEVES, Iêdo Batista. Vocabulário prático de tecnologia jurídica e de brocados latinos. 4. ed. Rio de Janeiro, Fase, 1991. 473p.

32 NIGRI, Deborah Fisch. Crime e informática: um novo fenômeno jurídico. In: Revista Trimestral de Jurisprudência dos Estados. v. 16, n. 100, p. 41-48, mai 1992.

33 NORONHA, Edgard Magalhães. Direito penal. 20. ed. São Paulo : Saraiva, 1992. v.I-IV

34 PALADINO, Enzo. Novo dicionário técnico de informática. São Paulo : Ciência Moderna, 1986. 458p.

35 PRADEL, Jean. Les infractions relatives a l'informatique. In: Revue Internationale de Droit Compare, Paris (France), v. 42, n. 2, p. 815-828, juin 1990.

36 Sexo 'on line' nos EUA seduz adolescentes e desafia a censura. O Globo, Rio de Janeiro, 9 jul 1995, p. 50.

37 TEODORO JUNIOR, Euclides. Computador a serviço do crime. In: BANAS. São Paulo, v. 25, n. 1192, p.30-32, dez 1978.

DEDICATÓRIAS

A minha esposa Jane pelo amor e compreensão.

Aos meus filhos, Êmerson e Camila, por terem compreendido a minha ausência nestes cinco anos.

E ao meu pai, doce lembrança.

AGRADECIMENTOS

Ao Dr. Derocy Diácomo Cirillo da Silva, pelo acesso aos bancos de pesquisa da Procuradoria da República no Rio Grande do Sul.

Ao Dr. Edison Gomes Machado, o mestre e amigo de todas as horas.

Ao Dr. José Guilherme Falleiro, pela cooperação imprescindível.

Ao Dr. João Sidnei Duarte Machado, pelas horas de dedicação ao nosso trabalho como também as preciosas críticas e sugestões.

Ao Dr. Luis Machado Stabile, pelo apoio técnico a este trabalho.

Ao Dr. Mauro Fonseca Andrade, pela cooperação inestimável.

Ao Dr. Pacífico Luiz Saldanha, pelas primeiras lições jamais esquecidas de Direito Penal e orientação segura deste trabalho.

Ao Prof. Protásio Pletsch, pela dedicação aos nossos objetivos.

À bibliotecária Regina Iara Machado dos Santos, pela pesquisa e solicitude no fornecimento de material bibliográfico da Procuradoria da República no Rio Grande do Sul.

Ao Antonio Cândido Mendes de Souza, o amigo nos momentos mais difíceis.

* advogado em Uruguaiana (RS)