Crime Informático

Álvaro Mayrink da Costa
Desembargador do TJ/RJ. Professor da EMERJ e do Curso de Mestrado da Universidade Cândido Mendes

1. Generalidades

A macrossociedade sofre profundas modificações no plano psicossocial, econômico e político, nos tempos contemporâneos, cujos efeitos nas áreas anômicas ocorrem de forma impressionante; todavia, no plano do ser, torna-se difícil medir os efeitos que irão gerar na primeira década do novo século.

Anota-se, no campo do direito, reflexos que se tornaram constantes desafios aos doutrinadores, legisladores e aplicadores da lei.Tais fenômenos, especialmente focados nos campos da informática e das telecomunicações, diante da globalização, ultrapassam os limites nacionais, trazendo uma interdependência entre os povos do planeta e, como tal, diante dos conflitos globais, uma criminalidade transnacional.

Como operadores do direito, podemos inicialmente vislumbrar vertentes que se constituem a partir da separação do meio e mensagem, do aumento do poder decisório do indivíduo, do maior destaque às etnias e realidades regionais e na busca permanente do objetivo da integração internacional.

A título de ilustração, citaríamos o meio e a mensagem na evolução histórica da humanidade com as grandes mudanças, das quais tem maior realce sem dúvida, a informação, a qual acarreta problemas jurídicos vinculados aos atos realizados à distância ou através de equipamentos eletrônicos.

Outrossim, os avanços da tecnologia permitem à pessoa humana, isoladamente, buscar a informação onde melhor lhe aprouver. Daí surge uma pluralidade de comportamentos que escapam aos controles normativos.

Por último, desde a Revolução Francesa, com o desenvolver de um mito universalista, a história da humanidade no mundo atual procura uma sintonia com interesses próximos da realidade em razão de tradições e experiências regionais; há, pois, a constante perda de uma visão universalista pela ampliação de um universo regionalista (Comunidade Européia, Mercosul, Nafta etc.), isto é, a procura da formação de blocos integrando realidades distintas, mas complementares.

2. A macrossociedade e a revolução cibernética

É evidente a mudança no conceito clássico de soberania, na proporção da tendência atual da união de complementariedade na formação de blocos, grupos e mercados comuns identificando-se com os interesses da comunidade internacional.

Com a tecnologia, em destaque a informática, a pessoa humana deixou de ser uma figura abstrata, de ser um objeto em um processo político, constituindo-se em um verdadeiro ator que inaugura um plurirrelacionamento com outras pessoas humanas em qualquer parte do planeta, abstraindo-se de ter ou não conhecimento.

A crise conceitual da soberania sob o enfoque clássico deve-se à informática e as telecomunicações, visto que não temos mais uma sociedade circunscrita a um limite territorial, mas uma macrossociedade global, que em suas trocas muitas vezes atua anomicamente. Perdem a eficácia os provimentos judiciais diante das novas realidades, em nossa área indicando-se, como exemplo, o crime organizado, o que requer a criminalização de novos comportamentos, como a lavagem de dinheiro, gerando a necessidade da modificação das legislações regionais diante da nova realidade global. Há a exigência, por força de tal realidade virtual, de ser redefinido o perfil do comportamento do indivíduo e dos grupamentos sociais. O desafio do operador do Direito, no plano do ser, está no reconhecimento de novos instrumentos de comunicação e informação para capacitar, no campo do dever-ser, observado o mínimo de intervenção, impondo ao legislador penal, na criação de modelos, para dar garantia através de novas figuras, a vida dos indivíduos na macrossociedade.

Assim, é do consenso geral que o computador se constituiu na inovação tecnológica mais importante do nosso tempo, no que se

denominou na década de 80, de revolução cibernética. De um lado, vislumbra-se a fonte do poder, pois quem utiliza a informática recebe mais rapidamente informações, formando um maior universo de conhecimentos.

Não podemos olvidar, nos reflexos gerados diante dos avanços da informática, as vulnerabilidades pertinentes à autenticidade, à integridade, à confiabilidade e, como requisitos formais, à eficácia e validade dos documentos virtuais.

3. O documento eletrônico

Anotamos, no campo formal, o óbice relativo à autenticidade do documento ou da mensagem, produzidos ou transmitidos remotamente (*home banking*). É relevante a validade do documento eletrônico, bastando exemplificar que a mensagem enviada por *e-mail* dificilmente terá validade jurídica plena, equiparando-se à prova oral pois, através de recursos técnicos, há possibilidade da alteração de documentos digitais sem deixar vestígios. A equiparação do documento eletrônico ao documento físico escrito e assinado (art. 368 do CPC.) deve estar certificada digitalmente por meio da criptografia assimétrica, caso contrário, teríamos um contrato cuja forma se assemelharia à forma verbal.

Para Carnelutti, a assinatura escrita possui três funções elementares: *indicativa, declarativa e probatória*. A nosso aviso, o conceito de documento é amplo, admitindo a representação livre dos fatos, atos e manifestações da vontade. O documento eletrônico é admitido nos países de sistema de livre apreciação, devendo o julgador atribuir os efeitos e a força probatória, após precisa valoração da comprovação de sua autenticidade. Não podemos olvidar, diante do art. 335, do CPC., e na falta de normas jurídicas particulares, que o julgador deverá aplicar as regras da experiência comum subministradas pela observação do que originariamente acontece no cotidiano da vida e, ainda, as regras emanadas da experiência técnica, ressalvado, quanto à esta, o exame pericial, trilhando-se pelo princípio da livre apreciação judicial da prova.

4. Criptologia

A legislação brasileira tem caminhado. A Medida Provisória nº 2.200, de 28 de junho de 2001, que instituiu a Infra Estrutura de Chaves Públicas Brasileiras, veio a dar a garantia da comunicação com órgãos públicos por meios eletrônicos. Dos projetos apresentados, o mais completo é o projeto n.º 1.589/99, de iniciativa da OAB, através do qual propõe a equiparação do "*documento eletrônico assinado pelo seu autor, mediante sistema criptográfico de chave pública*".

Objetivando assegurar a privacidade, a identidade da autoria e a inalterabilidade do conteúdo em relação à segurança dos contratos virtuais surgiu a criptologia, representativa da codificação de informações de forma a impedir a intercepção não desejada através de convenções secretas às partes contratantes e às testemunhas. Recorde-se que a mensagem é criptografada na origem e o destinatário recebe uma chave que serve tanto para codificação como para a descodificação. O sistema de utilização de chaves *públicas* e *privadas* garante o sigilo das transações ocorridas em rede e possibilita a identificação do remetente e do receptor, pois é atribuída ao remetente uma chave privada, de seu exclusivo conhecimento, enquanto o destinatário deverá saber a chave pública, correspondente à chave privada do remetente, única que tem a possibilidade de decodificar a mensagem enviada. Portanto, a utilização da chave privada quase se assemelha a àssinatura eletrônica. O conceito de mensagem para o computador refere-se a um banco de dados, armazenado em arquivo seguro, transmitido via digital. (*Eletronic Data Interchange – EDI.*).

5. Assinatura digital

O Anteprojeto de Lei n.º 158/99, encaminhado pelo Deputado Federal Michel Temer, acolhe a criptografia assimétrica como linguagem segura para caracterizar a assinatura digital e constituir o documento eletrônico. Na esteira de Raimundo Zagami, "Uma firma digital é um conjunto de caracteres alfanuméricos resultantes de complexas operações de criptografia efetuadas por um computador sobre documentos eletrônico"[1]. A validade das assinaturas eletrônicas

[1] N.R. Renato M. S. Olice Blum, "O Processo Eletrônico: Assinaturas, Documentos e Instrumentos Digitais", *in* **A Internet e os Tribunais**, São Paulo, Edipro, 2001.

constitui a questão de maior relevo. A assinatura digital não é uma assinatura diante do modelo do inciso II, do art. 585, do CPC., sendo conferida pela criptografia, através de suas chaves e certificados. Nos dias atuais, as senhas bancárias ou de cartões de pagamento são identificadoras dos pólos da relação jurídica, sendo intermediária da operação a Instituição Financeira depositária dos códigos e a capacidade do pagador. Quem assina a senha é o seu detentor. Portanto, a assinatura eletrônica é a realizada em forma de sinal, marca ou código identificador de determinada pessoa em uma operação certificada de forma eletrônica. O documento eletrônico não é usualmente assinado de próprio punho, mas pode-se seguramente aferir a autenticidade da assinatura digital, a qual possui cunho declarativo e constitutivo de direito e obrigações.

6. Autenticidade do documento eletrônico

A assinatura digital por uma chave privada e uma chave pública (criptologia assimétrica) é a mais segura, sendo necessário que exista uma autoridade certificadora que emitirá um *certificado* contendo a chave pública do usuário, e esse certificado acompanhará os documentos eletrônicos assinados, dando características básicas de autenticidade. As características essenciais da assinatura assimétrica são: a) autenticidade do documento para a geração de efeitos jurídicos; b) impossibilidade de falsificação porque só o subscritor tem a chave que possibilita assinar o documento; c) vedação de utilização em novo documento; d) impossibilidade de modificação das características do documento depois de assinado pelo autor e vedação de contestação, desde que empregado um sistema aprovado e esteja certificado o documento.

Já podemos aferir autenticidade da assinatura no instrumento, no papel utilizado, em função do documento de identidade, diante de laudos técnicos e verificação estática. Busca-se superar a vulnerabilidade em tema tão importante sincronizando a autenticidade do documento e da mensagem do agente produtor, emissor ou receptor. Não se olvide que identidade do autor é elemento fundamental na sociedade virtual. A assinatura digital está associada a uma senha que habilita o usuário a certas operações, é uma assinatura por ficção, que dependeria de norma expressa e não de mera

previsão contratual ou de praxe comercial. A assinatura e as testemunhas são figuras ligadas a átomos, daí o desafio. Não se oblitere que a senha (*password*), constitui conjunto de caracteres que pode ser numérico ou alfanumérico, utilizado para proteger as informações sigilosas de pessoas não autorizadas, podendo ser agrupadas em senhas de acesso e na denominada assinatura digital. O acesso (entrar, ingressar, encontrar, iniciar), significa que a pessoa está entrando em contato com as informações do banco de dados. Há sempre o risco da *clonagem* de cartões eletrônicos, que se dá pela cópia do que se encontra na sua tarja magnética ou pelo acesso aos computadores centrais das entidades financeiras ou de crédito. As senhas são seqüências de *bits,* e aquele que tiver a sua posse terá acesso às informações. Daí a necessidade de instrumentos para enfrentar este novo modelo de criminalidade (senhas, certidão e autentificação, criptografia e esteganografia).

7. A criminalidade informática

A criminalidade informática oferta as mesmas características da informatização global; senão vejamos: *a transnacionalidade* (todos os países fazem uso da informática independentemente do seu estágio econômico, social ou cultural) e portanto, o injusto penal se encontra em toda sociedade global; *a universalidade* (todas as pessoas de qualquer plano econômico, social ou cultural têm acesso aos produtos informatizados); *a ubiqüidade* (a informatização está presente em todos os setores públicos e privados no planeta).

Assim, observamos a presença da informática como o mais novo e preponderante fator criminógeno, pois de um lado abre maior espaço aos infratores para o cometimento de injustos penais, utilizando-a como ferramenta eficaz, potencializando ilicitudes como estelionato, o racismo, a pedofilia e os crimes contra a honra; de outro, permite o cometimento de novas ilicitudes, exemplificando-se: a utilização abusiva da informação armazenada, violando o direito à privacidade, à intimidade e à imagem dos indivíduos. Em síntese, temos os injustos penais cometidos pelo uso do computador (*computer crime*), bem como contra o computador (*hardware, software*) ou mesmo contra a própria informação.

8. O momento consumativo

O momento consumativo do crime do computador exige a verificação do *iter* percorrido, salientando-se, para tanto, o momento da entrada dos dados (*input*), a programação dos dados, o processamento dos dados, a saída dos dados (*output*) e a comunicação eletrônica. Significa dizer que o *iter* exige a verificação do planejamento, preparação, execução, consumação, com ou sem exaurimento, onde se inclui a destruição de provas.

9. Culpabilidade

Questão polêmica diz respeito à capacidade de culpabilidade, mais especificamente, à imputabilidade como pressuposto da culpabilidade. A dificuldade está em se identificar o autor do ato nas transações eletrônicas. E, no campo da responsabilidade civil, a culpa *in vigilando* (ausência do dever de cuidado na guarda de senha de acesso). A culpa *in eligendo* assume relevância especial no caso de contratações de bens e serviços da informática. E a culpa *in omittendo* caracteriza-se pela omissão de informações relevantes. Já a culpa *in custodiendo* pode-se configurar em relação à guarda de dados (recursos financeiros) que os clientes do banco fazem trafegar pela rede no âmbito da prestação de serviços; por último, a culpa *in contraendo* situa-se nas condições em que o banco se encontra no momento da oferta dos seus serviços. Não podemos olvidar o respeito à integridade dos documentos e das mensagens, e o da confiabilidade das comunicações que transitam na comunicação à distância através de rede de computadores[2]. O sigilo informático é uma preocupação de todos (grampeamento das comunicações, gravações ou cópias não autorizadas das mensagens, dados, documentos e informações enviadas eletronicamente).

Uma das grandes vulnerabilidades no combate à criminalidade informática é a ausência de dados empíricos, calculando-se a *cifra negra* em noventa e oito por cento (98%), indicando-se como fatores para seu alto percentual: a dificuldade probatória, a desconfiança da vítima na eficácia do sistema judicial, na aparência de legalidade do comportamento dos atores, e a pouca visibilidade diante do anonimato.

[2] Art. 5.º, inciso XII, da Carta Política de 88.

10. Perfil de sujeitos

Aspecto relevante para o criminólogo é o perfil dos sujeitos no crime do computador, pois o sujeito ativo, quer de direito público ou privado, via de regra é pessoa jurídica de grande poder econômico, que não comunica o ato de que foi vítima, alimentando o sistema de impunidade e o crescimento do comportamento ilícito.

11. Características do atuar reprovável

O sujeito ativo, pessoa física, está mais distante do glamour do *hacker* estudante de classe média acreditando-se genial com alta especialização informática. Os tempos românticos já passaram. Os delinqüentes são pessoas que trabalham preferencialmente no ramo informático, empregados, e seu perfil acusa pouca temibilidade em relação à norma, insensibilidade à reação penal, motivado pelo animo de lucro, perspectiva de promoção, vingança ou tão-só para chamar a atenção.

São características do atuar desvalorado: a alta lesividade econômica, a conduta realizada em local distante do resultado (crime plurilocal), e a reiteração freqüente (crime continuado). Recorde-se que, quanto ao *lugar do crime,* a soberania dos Estados impõe a aplicação da lei penal em todo o seu território, ocorrendo situações que ultrapassam a sua fronteira, o que normalmente ocorre nos *crimes do computador*, principalmente com a utilização da *internet*. O nosso Código penal adotou, em seu art. 5º, o princípio da territorialidade como regra e, como exceções, os princípios da defesa (art. 7º, I e par. 3º), da justiça universal (art. 7º, alínea *a*) da nacionalidade (art. 7.º, inc. II, alínea *b*) e da representação (art. 7.º, II, alínea *c*). O Código brasileiro adotou a teoria da ubiqüidade para delimitar o local do crime. É comum o crime à distância, aquele em que a conduta é praticada fora do país e o resultado aqui ocorre, ou vice versa. Na prática, é necessário identificar-se o local da ação e do resultado.

Como vimos, o controle da criminalidade é altamente seletivo (*labelling approach).* Infelizmente, nos tempos atuais a impunidade o caracteriza, visto que não se trata de crime ostensivo, havendo complexidade técnica dos sistemas informáticos, o domínio da tecnologia, a confiança no computador, a falta de documentos escri-

tos das operações, a insuficiência de medidas de segurança e controle, a característica dos crimes plurilocais, a difícil prova da autoria, o medo da vítima de que durante o processo seja descoberto segredo empresarial.

12. Bem jurídico

No que concerne ao bem jurídico várias classificações são propostas, sendo que Bassiouni, à luz do Direito Penal Internacional, sugere: **a** – crimes que violam direitos à privacidade e outros direitos humanos; **b** – crimes que importam em novas formas de criminalidade econômica; **c** – crimes que representam perigos à segurança nacional. Não podemos esquecer o desafio neste novo campo do direito sob um aspecto multifacetado: **a** – tutela legal dos instrumentos informáticos; **b** – proteção da intimidade e de dados reservados; **c** – contratos informáticos; **d** – responsabilidade civil por danos emergentes da informática; **e** – delitos instrumentados mediante o uso do computador. Na busca da conceituação duas vertentes nos direcionam, uma dada pela Organização para a Cooperação Econômica e o Desenvolvimento (OCDE) que considera o delito informático (*computer crime*) qualquer conduta ilegal, não ética e não autorizada que viole o processamento automático de dados e/ou a transmissão de dados; a outra, por Tiedemann (1985), de que a criminalidade mediante computadores alude a todos os atos antijurídicos realizados com emprego de um equipamento automático de processamento de dados.

É certo que as modalidades delitivas tradicionais existentes antes da aparição do computador e agora realizadas por meio de sua utilização incrementaram as taxas de aumento da criminalidade com rapidez e impunidade.

13. Classificação típica

Podemos classificar os crimes do computador em puros e impuros, ou próprios e impróprios. Na verdade, os verdadeiros *computer crimes* são os puros ou próprios, pois os impuros ou impróprios são os crimes comuns realizados por *meio do computador*.

A classificação varia desde a baseada em Martine Briat, Ulrich Sieber e Marc Jaeger, para citarmos as mais tradicionais. A orientação

da legislação portuguesa, a nosso sentir, mais se alinha aos objetivos colimados (crimes ligados à informática): **a** – falsidade informática; **b**- dado relativo a dados ou programas informáticos; **c** – sabotagem informática; **d** – acesso ilegítimo; **e** – interceptação ilegítima; **f** – reprodução ilegítima de programa protegido. A legislação portuguesa elenca entre as penas aplicáveis às pessoas coletivas equiparadas: **a** - a admoestação; **b** – multa; **c** – dissolução; e entre as penas acessórias: **a**- perda de bens; **b** – caução de boa conduta; **c** – interdição temporária do exercício de certas atividades ou profissões; **d** – encerramento temporário do estabelecimento; **e** – encerramento definitivo do estabelecimento e **f** - publicidade da decisão condenatória. Em disposições finais, transitada em julgado a decisão, aplica-se a pena de dissolução através de processo de liquidação. Em relação à pessoa humana aplica-se a pena de prisão e a pecuniária.

A nosso sentir, a legislação portuguesa é a mais bem sistematizada normativamente. No direito pátrio os crimes informáticos puros e impuros, tipificados no Código penal e nas leis especiais podem ser anotados: **1** - crimes contra a honra (arts. 138, 139 e 140 do CP. e na Lei n.º 5.250/67, que regulam a liberdade de manifestação do pensamento e informação em seus arts. 20, 21 e 22; todos tratam dos tipos de calúnia, difamação e injúria. Em se tratando de crime de imprensa, a competência será o local da sede da empresa responsável pela divulgação, podendo ser a empresa construtora do *site* ou a que presta manutenção); **2** – crime de ameaça (art. 147 do CP.); **3** – (*puro*) intercepção de *e-mail* (art. 151, do CP., Lei n.º 9.296/96 que regula o inciso XII, parte final do art. 5.º da Constituição e que prevê no seu art. 10.º/: "*constitui crime realizar interceptação de ligações telefônicas de informática, ou telemática, ou de quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei*".). O Código Penal brasileiro trata no inciso III do § 1º do art. 151 da *Violação de comunicação telegráfica, radioelétrica ou telefônica*, cujo objeto jurídico é a liberdade individual especialmente garantida no art. 5º XII da Carta da República, com as exceções no estado de defesa (art. 136, § 1º, I, *b* e *c*, 1ª parte) ou de sítio (art. 139, III). O exercício regular de um direito e o estado de necessidade justificante são justificantes do obrar típico (ainda: art. 10 da Lei nº 6538, de 22-6-1978), podendo ocor-

rer o erro de tipo ou de proibição. Poderá ocorrer *espionagem* contra interesses potegidos pela Lei de Segurança nacional (art. 13 e 14 da Lei nº 7.170 de 14-12-1983), como também *abuso de autoridade* (arts. 13 e 14 da Lei nº 4898 de 9-12-1965). Aduza-se que na violação de *e-mail* há busca e apreensão do computador determinado pela autoridade, devendo serem periciados o computador, programas e arquivos, mas os *e-mails* ficam garantidos pelo sigilo; **4** – (puro) interceptação de *e-mail* comercial (art. 152 do CP. e art. 10.º da Lei 9296/96); **5** – divulgação de segredo (art. 153 do CP., dando-se destaque ao parágrafo 1.º - A: "*Divulgar, sem justa causa, informações sigilosas ou reservadas assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública*", acrescentado pela Lei nº 9.983/2000). O citado diploma fez inserir o § 1º, inciso I do Art. 325 do CP ("*permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informação ou banco de dados da Administração Pública*"). Nas modalidades de *permitir* ou *facilitar*, a ação pode ser comissiva ou omissiva, ao passo que na de utilizar, será sempre comissiva. O particular pode ser co-autor ou partícipe, desde que saiba da condição de funcionário público do autor; **6** – furto (at. 155 do CP.) **7** – (*puro*) envio de vírus e similares (art. 163 do CP.); **8** – apropriação indébita (art. 168 do CP); **9**– estelionato (art. 171 do CP., dando-se destaque à expressão normativa "*qualquer outro meio fraudulento*"); **10** - violar direito autoral (art. 184 do CP); **11** – escárnio por motivo de religião (art. 208 do CP); **12** – favorecimento da prostituição (art. 228 do CP); **13** – ato obsceno (art. 233 do CP); **14** – escrito ou objeto obsceno (art. 234 do CP); **15**- incitação ao crime (art. 286 do CP); **16** – apologia de crime ou criminoso (art. 287 do CP); **18** – (*puro*) inserção de dados falsos em sistema de informações (Lei nº 9.983, de 14/7/2000). Somente o funcionário público pode ser sujeito ativo, sendo a administração pública o sujeito passivo (art. 313 – A, do CP): *"Inserir ou facilitar, o funcionário público autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem para causar dano."* Há, pois, quatro condutas típicas:

a) *inserir* (introduzir, incluir) dados falsos; **b**) *facilitar* (tornar fácil, auxiliar, afastar dificuldade) a inserção de dados falsos; **c**) *alterar* (mudar, modificar) indevidamente dados corretos; **d**) *excluir* (eliminar) indevidamente dados corretos. O dolo é com especial fim de agir. O particular pode ser co-autor ou partícipe do delito, apesar de ser tipo próprio, se tinha conhecimento da condição de funcionário *autorizado* do autor; **19** – (*puro*) modificação ou alteração não autorizada de sistema de informação (Lei nº 9.983 de 14/7/2000. – art. 313 – B, do CP): "*Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente*". Não há exigência de ser funcionário autorizado. No caso o dolo é genérico, bastando que modificação ou alteração seja realizada sem a autorização da autoridade competente. O particular pode ser co-autor ou partícipe, sabendo da condição de funcionário público do autor. O sistema de informação ou o programa de informática deverá ser da Administração Pública; **20** – jogos de azar (art. 50 da LCP e art. 75 da Lei n.º 9.615/98 – Bingo irregular); **21** – pedofilia (art. 241 do ECA, cuja redação foi alterada pela Lei 10.764 de 12.11.2003, ficando "*apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação inclusive internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente*", passando a abranger de modo específico a pornografia infantil na internet. Aduza-se que a Lei 10.764 ainda produziu outras alterações no art. 241 do ECA, tais como: "*assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens*" ou ainda, "*assegura, por qualquer meio, o acesso na rede mundial de computadores ou internet, das fotografias, cenas ou imagens*" de sexo explícito produzidas com a participação de crianças ou adolescentes. O legislador procurou responsabilizar o provedor de serviço de hospedagem de página *web* e o provedor de serviço de acesso à internet, sempre que contribuam para a divulgação de pornografia infantil. Questão em aberto fica a chamada "pornografia infantil virtual", entendida como o material visual que aparentemente descreve cenas de menores envolvidos em relações sexuais explícitas, mas que na verdade é produzido sem a participação real de crianças ou adolescentes. **22** – crime de discriminação ou preconceito de raça, cor,

etnia, religião ou procedência nacional (art. 1.º e 20.º da Lei 7.716/89); **23** – (*puro*) interceptação de comunicação telefônica ou telemática (art. 10º da Lei 9.296/96); **24** – crimes contra a segurança nacional (arts. 22 e 23 da Lei nº 7.170/83); **25** - crimes contra a propriedade industrial (Lei 9.279/96, com destaque para o art. 195 - Concorrência desleal); **26** – crimes de lavagem de dinheiro (art. 1.º da Lei 9.613/98); **27** – (*puro*) violação da proteção intelectual de programa de computador e sua comercialização (art. 1.º e 12.º da Lei n.º 9.609/98 – Lei do *software*). A CPI da pirataria, em seu relatório final, identifica atos e sugere a incriminação em relação a reprodução de programas de computadores, obra intelectual, CDs, DVDs e vídeo.

14. Conclusão

Há condutas ofensivas aos sistemas informáticos ou telemáticos ou mesmo pertinentes ao uso do computador que não se adequam às figuras penais descritas em nossa legislação, que estão a exigir, observado o Direito Penal mínimo, a imediata criminalização (dano de sistemas informáticos e telemáticos, atentado a equipamentos de utilidade pública, falsificação, alteração ou supressão do conteúdo de comunicações informáticas ou telemáticas, difusão de programas que visem a danificar ou interromper um sistema informático, dano relativo a dados ou programas informáticos, sabotagem informática).

A idéia de tempo *diferido* (tempo dos fusos horários, das etapas lógicas e sucessivas), graças à velocidade das comunicações, cede lugar a idéia de *tempo real* (tempo das comunicações virtuais e instantâneas, incompatível com a relação passado, presente e futuro).

Logo, podemos observar que a questão adquiriu corpo, intensidade e atualidade, na proporção em que a ordem econômica e o respeito à dignidade da pessoa humana transnacionalizada causam prejuízos vultosos.

Por fim, não se pode admitir a proliferação de comportamentos reprováveis perante as legislações mais avançadas no campo do direito

comparado, quando já acordado pelo Brasil a sua incriminação (*puros*), gerando a impunidade diante deste novo modelo de criminalidade.

Concluindo, não podemos deixar de citar o imortal Charles Chapplin, quando afirma: "*Mais do que de máquina, precisamos de humanidade. Mais que inteligência, precisamos de afeição e doçura. Sem essas feições a vida será de violência e tudo será perdido*".◆

Consulte-se: **Direito & Internet, Aspectos Jurídicos Relevantes**, Coordenadores – Newton de Lucca e Adalberto Simão Filho, IBCI, EDIPRO, - 2000; **Comércio Eletrônico**, Organizadores – Ronaldo Lemos da Silva Junior e Ivo Waisberg, Co-edição, IASP e RT, 2001; **Direito Eletrônico**, Coordenador Renato Opice Blum, **A Internet e os Tribunais**, EDIPRO, 2001; **Internet o Direito na Era Virtual**, Luís Eduardo Schoueri, Organizador, 2.ª, ed. Forense, 2001; Marco Aurélio Greco, **Internet e Direito**, Dialética, SP, 2000; Liliana Minardi Paesani, **Direito e Internet**, Atlas, 2000; Luis Henrique Ventura, **Comércio e Contratos Eletrônicos, Aspectos Jurídicos**, EDIPRO, 2001; Aluízio Ferreira, **Direito à Informação – Direito à Comunicação, Direitos Fundamentais na Constituição Brasileira**, Celso Bastos Editor, 1997; Carla Rodrigues Araújo de Castro, **Crimes de Informática e seus Aspectos Processuais**, Lumen Juris, 2001; Maria Helena Junqueira Reis, **Computer Crimes – A Criminalidade na Era dos Computadores**, Del Rey, 1997.