Túlio Lima Vianna

DO ACESSO NÃO AUTORIZADO A SISTEMAS COMPUTACIONAIS:

fundamentos de Direito Penal Informático

Dissertação apresentada ao Curso de Mestrado da Faculdade de Direito da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Direito.

Área de concentração: Ciências Penais

Orientador: Prof. Dr. Ariosvaldo Campos Pires

Belo Horizonte

Faculdade de Direito da UFMG

2001

Dissertação defendida e aprovada, em 04 de setembro de 2001, pela banca examinadora constituída pelos professores; média final igual a 9,-

Prof. Dr. Ariosvaldo Campos Pires – Orientador

Prof. Dr. Jair Leonardo Lopes

Prof. Dr. Wagner Meira Júnior

À Cynthia Semíramis, com amor.

Ao Prof. Ariosvaldo Campos Pires – profissional respeitado nas tribunas e querido nos bancos escolares – pela amizade e maestria na orientação deste trabalho.

Ao Juiz Erony da Silva – magistrado honrado e precursor de um novo tempo – pela confiança e estímulo no cotidiano profissional.

Ao Prof. Virgílio Mattos – mestre, colega, amigo!
Em sua genialidade, escreve sobre criminosos loucos;
serei eu louco por escrever sobre gênios do crime?
Penso ter aprendido as lições...

The Conscience of a Hacker [1]

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world... Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike.

A consciência de um Hacker [2]

Prenderam outro hoje, está em todos os jornais. "Adolescente preso no Escândalo do Crime Informático", "Hacker Preso após Invadir Banco"... Malditos garotos. São todos iguais.

Mas você, com sua elegante psicologia e cabeça dos anos 50, alguma vez já olhou no fundo dos olhos de um hacker? Alguma vez indagou-se sobre o que o motivou, que forças o formaram, o que teria o moldado? Eu sou um hacker, entre em meu mundo... Meu mundo é um mundo que começa na escola... Eu sou mais esperto que a maioria das outras crianças, esta merda que nos ensinam me irrita... Malditos fracassados. São todos iguais.

Eu estou no científico. Ouvi os professores explicarem pela qüinquagésima vez como se reduz uma fração. Eu entendo. "Não Sra. Smith, eu não demonstrei meus cálculos. Eu os fiz de cabeça..." Maldito garoto.

---

[1] MENTOR, The. *The conscience of a hacker.* Disponível em: <http://www.attrition.org/~modify/texts/ethics/hackers_manifesto.html>.

[2] Tradução livre nossa.

all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty

Provavelmente colou. São todos iguais.

Fiz uma descoberta hoje. Eu descobri o computador. Espere um segundo, isto é legal. Ele faz o que eu mando. Se comete um erro, é porque eu o obriguei a isso. Não porque não goste de mim... Ou se sinta ameaçado por mim... Ou pense que eu sou um c.d.f. ... Ou não goste de ensinar e não devesse estar aqui... Maldito garoto. Tudo que ele faz é jogar. São todos iguais.

Então aconteceu... uma porta abriu-se para o mundo... correndo pela linha telefônica como heroína nas veias de um viciado, um comando é enviado, uma fuga da incompetência do dia-a-dia é procurada... Uma BBS é achada. "É isto... aqui é meu lugar..." Eu conheço todos aqui... mesmo aqueles que nunca encontrei, com quem nunca conversei, e talvez jamais torne a escutá-los... Eu sei quem são... Maldito garoto. Interrompendo a linha telefônica de novo. São todos iguais...

Quer apostar seu cu que somos todos iguais... fomos alimentados com comida de bebê na escola quando estávamos famintos por bifes... os pedaços de carne que deixaram escapar estavam já mastigados e insípidos. Fomos dominados por sádicos ou ignorados por indiferentes. Os poucos que tiveram algo a nos ensinar encontraram em nós discípulos fiéis, mas foram raros como lagos no deserto.

Este é nosso mundo agora... o mundo

of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

Written on January 8, 1986

do elétron e do comutador, a beleza do baud. Usamos um serviço já existente sem pagar por aquilo que poderia ser baratíssimo se não fosse explorado por especuladores insaciáveis, e vocês nos chamam de criminosos. Nos exploram... e nos chamam de criminosos. Buscamos conhecimento... e nos chamam de criminosos. Somos sem cor, sem nação, sem preconceitos religiosos... e nos chamam de criminosos. Vocês constroem bombas atômicas, declaram guerras, assassinam, trapaceiam e mentem para nós e tentam nos fazer crer que é para nosso próprio bem, e ainda assim os criminosos somos nós.

Sim, sou um criminoso. Meu crime é a curiosidade. Meu crime é julgar as pessoas pelo que dizem e pensam, não pelo que aparentam ser. Meu crime é ser mais inteligente que vocês, algo pelo que jamais irão me perdoar.

Eu sou um hacker, e este é meu manifesto. Vocês podem parar este indivíduo, mas não poderão parar todos nós... afinal, somos todos iguais.

+++ O Mentor+++

Escrito em 8 de janeiro de 1986

SUMÁRIO

RESUMO

A necessidade de tipificação do acesso não autorizado a computadores na legislação penal brasileira é o objeto de estudo do presente trabalho. Trata-se de pesquisa multidisciplinar na qual procurou-se identificar o significado jurídico penal de uma série de conceitos fundamentais da Ciência da Computação. A abordagem do tema é pioneira nos cursos de pós-graduação *stricto sensu* do país e buscou suprir a imensa lacuna existente na bibliografia nacional.

A garantia constitucional à inviolabilidade da intimidade e da vida privada, consagrada no art. 5º, X, da Carta Magna tem como corolário a tutela jurídico-penal do bem jurídico inviolabilidade dos dados informáticos. Partindo-se de tal pressuposto, procurou-se demonstrar a necessidade de tipificação na legislação penal brasileira da conduta de acessar sem autorização sistemas computacionais. Este delito foi classificado como crime informático próprio e sua distinção em relação aos demais delitos do gênero foi realizada com base no bem jurídico tutelado.

Procurou-se identificar, através de um breve estudo criminológico, os diversos comportamentos dos criminosos tecnológicos, para uma compreensão geral do problema. A legislação estrangeira de mais de dez países foi analisada e suas principais virtudes e equívocos foram comentados. O verbo típico e os elementos normativos do tipo foram estudados, procurando-se fixar os limites da conduta típica, com o reconhecimento, inclusive, da possibilidade da aplicação do Princípio da Insignificância em alguns casos.

Capítulo especial foi destinado à determinação do momento e do local de ocorrência do delito, bem como à fixação do juízo competente para o conhecimento e julgamento das ações penais nos delitos informáticos. O *iter criminis* foi examinado em todas as suas fases, e reconheceu-se a possibilidade da tentativa. Os sujeitos ativo e passivo também foram analisados, com especial comentário a respeito da possibilidade de se responsabilizar penalmente a pessoa jurídica responsável por crimes informáticos. Os casos de concurso de agentes foram comentados com base tanto na teoria formal-objetiva, como na teoria do "domínio do fato", procurando-se determinar qual delas melhor se adapta ao caso concreto.

Em nossas conclusões apresentamos uma proposta de lei que visa a disciplinar a matéria, seguida dos comentários resumidos de tudo aquilo que foi examinado no corpo do texto.

Complementam o trabalho os anexos com a íntegra das legislações estrangeiras pesquisadas e os projetos de lei sobre criminalidade tecnológica da União Européia e do Brasil, este último em tramitação no Congresso Nacional. Acrescentamos ainda as telas das principais páginas brasileiras que foram vítimas de acessos não autorizados a sistemas computacionais como forma de ilustrar o potencial ofensivo dos piratas.

O anexo em CD-ROM traz a íntegra de todos os documentos consultados na Internet, inclusive os Códigos Penais completos de diversos países, tudo com o intuito de facilitar novas pesquisas sobre o tema.

Enfim, procurou-se reunir na presente pesquisa o maior número de informações possível, a fim de fornecer subsídios não só para uma correta tipificação do delito, mas também para sua eficiente aplicação futura pelo Poder Judiciário brasileiro.

PROLEGÔMENOS

Há cerca de quinhentos anos a Europa estendia suas fronteiras até um mundo novo. As grandes navegações foram um marco na história da humanidade, numa época em que navegar era antes de tudo um ato de coragem. Num oceano cheio de perigos naturais, talvez o maior dos desafios para os desbravadores dos mares fosse a mesma tecnologia que os movia. A então moderna engenharia náutica que permitia ao homem cruzar o oceano também permitia a aventureiros atacarem e saquearem embarcações. Esses facínoras dos mares ficaram conhecidos como piratas.

No século vinte e um, mais uma vez a humanidade prolonga suas fronteiras, não mais pelos mares que encantaram e ao mesmo tempo amedrontaram a humanidade, mas sim por um espaço não físico que se tornou conhecido como virtual. Um lugar que não é bom ou mau em si mesmo, mas tão somente um instrumento tecnológico colocado à disposição da humanidade que pode usá-lo bem ou mal. Um mundo que os norte-americanos chamaram de rede – Internet – mas pelo qual, curiosamente, navegamos – *browser*. Não nos causa surpresa que também aqui surjam os piratas.

Não se trata de mero capricho do vernáculo a identidade dos vocábulos. Em termos semânticos há muitas semelhanças entre os velhos piratas dos mares e

os modernos piratas virtuais[3]. Se tanto aqueles como estes são criminosos, forçoso também é admitir que são pessoas dotadas de inteligência e conhecimentos extraordinários para seu tempo. Se imaginarmos que um navegador antigo corresponderia a um astronauta contemporâneo, temos uma nítida imagem de que aqueles homens que enfrentavam tempestades, guiavam-se pelas estrelas, eram exímios espadachins e conheciam as línguas de diversas regiões não podem nem devem ser comparados a saqueadores de estradas.

Mutatis mutandis os piratas da atualidade também são pessoas de formação tecnológica bem acima da média, possuindo conhecimentos de informática, eletrônica e telefonia, dentre outros.

Piratas são os especialistas em radiofonia capazes de colocar no ar estações de rádio sem a devida autorização administrativa; piratas são especialistas em telefonia capazes de grampear centrais telefônicas inteiras e clonar celulares; piratas são os fraudadores de direitos autorais capazes de copiar programas de computador e, mais recentemente, discos de áudio; em suma, piratas são criminosos tecnológicos.

O termo pirata é também uma tradução bastante adequada para *cracker*, palavra originária da língua inglesa utilizada para designar indivíduos que

---

[3] Sobre a semelhança entre os antigos piratas e os modernos piratas virtuais e as diferenças entre os conceitos de *hackers e crackers* cf. SILVA NETO, Amaro Moraes e. *Resgatemos os hackers*. Disponível em: <http://www.jus.com.br/doutrina/hackers.html>.

acessam sem autorização sistemas computacionais.

Os piratas ou *crackers* não se confundem, no entanto, com *hackers*, apesar do uso indiscriminado das duas palavras pelos meios de comunicação.

A palavra *hacker* tem origem na língua inglesa – verbo *to hack* – e pode ser traduzida literalmente em português por talhar. Usada tradicionalmente para designar a atividade de lenhadores que talhavam a madeira, evoluiu semanticamente para designar qualquer golpe em um objeto.

> *"Según la leyenda, el primer uso no "tradicional" del término se debe a alguien que sabía donde dar el puntapié ("hack") exacto en una máquina de refrescos para conseguir una botella gratis. Ya sea en ese sentido o en el de cortar algo en pedazos, lo cierto es que el primer uso genuino de hacker en el mundo de la informática era el de alguien que conocía de forma tan detallada un sistema operativo (lo había "cortado en pedazos" por así decirlo) que podía obtener de él lo que quisiera (como el señor de la leyenda urbana acerca de una máquina de refrescos)."* (CASACUBERTA et al., 2000)

Em princípio a palavra era usada para designar qualquer pessoa que possuísse um conhecimento profundo de um sistema informatizado. Não tinha um sentido pejorativo, muito pelo contrário, ser considerado *hacker* era uma honra, uma vez que o vocábulo nomeava os respeitados especialistas da área de computação.

O termo evoluiu e atualmente é correntemente utilizado para designar os criminosos informáticos, já que efetivamente, tais indivíduos são *hackers* no sentido genérico da palavra, pois, para se invadir um sistema, necessário é que o agente possua um perfeito conhecimento de seu funcionamento.

No Brasil, o anglicismo já é registrado nos dicionários com o significado de:

> *"[Ingl., substantivo de agente do v. to hack, 'dar golpes cortantes (para abrir caminho)', anteriormente aplicado a programadores que trabalhavam por tentativa e erro.] S. 2 g. Inform. 1. Indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, ger. a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação."* (FERREIRA, 1999)

É possível que a palavra *hacker* acabe sendo incorporada ao vernáculo com este significado[4], mas melhor seria que fosse adotada em seu sentido original, isto é, para designar grandes especialistas na área de computação.

No jargão dos tecnólogos a palavra *hacker* ainda hoje é dificilmente usada com sentido pejorativo. Em geral, continua sendo empregada em seu sentido original para designar indivíduos profundamente conhecedores de sistemas operacionais, redes e linguagens de programação de baixo nível[5]. Ser considerado *hacker* é, para a maioria dos aficionados por computadores, um grande elogio.

O termo que melhor designaria os invasores de sistemas seria *cracker* ou, como sugerimos, sua tradução: pirata, termo que utilizaremos neste trabalho ao

---

[4] O aportuguesamento de um termo estrangeiro se faz pela transcrição fonêmica, razão pela qual a importação do vocábulo resultará necessariamente na mudança de sua grafia. Possivelmente admitir-se-á duas formas da palavra em questão: "ráquer", baseando-se na pronúncia equivocada, porém correntemente utilizada no Brasil e "réquer", respeitando-se a pronúncia original do verbo inglês *to hack*.

[5] Linguagens de programação de baixo nível são aquelas mais próximas da linguagem de máquina e, portanto, de mais difícil compreensão para o ser humano.

nos referirmos aos criminosos tecnológicos.

Piratas, *hackers* ou *crackers*, certamente tais designações seriam melhor estudadas por um lingüista que por um jurista, pois não se poderia criar uma norma que obrigasse às pessoas a falarem ou escreverem desta ou daquela forma. Deixemos que a evolução natural da língua nos mostre como devemos denominá-los.

Nossa meta aqui é fornecer subsídios para uma correta tipificação do acesso não autorizado a sistemas computacionais, analisando-o com base na Teoria do Delito e procurando, desde já, antecipar algumas das controvérsias jurisprudenciais que certamente surgirão com o advento da norma.

Frise-se, por fim, que este é um trabalho final do curso de mestrado, que tem como primordial objetivo a formação de professores universitários.

Seu escopo fundamental é, pois, ser didático, o que equivale a dizer que não se vislumbrará aqui a erudição própria das teses de doutorado, ainda que algo de conteúdo inédito efetivamente seja exposto.

Ocorre que é impossível dissociar o magistério da pesquisa e da extensão, visto que os grandes mestres são, e sempre foram, aqueles que ensinam, criam e aplicam o conhecimento. Impossível, pois, não procurar seguir este modelo.

Nossa proposta foi estudar um tema novo e de grande aplicabilidade prática, expondo da forma mais simples possível questões que, devido à sua multidisciplinariedade, apresentam-se muita vez como complexas.

Ao contrário de Nicanor Parra, que se dá por satisfeito com a compra de seus livros, este autor dar-se-á por realizado, tão-somente, com a leitura e compreensão desta obra.

1. Dos pressupostos conceituais

1.1. Objeto de estudo

Ao iniciarmos qualquer estudo científico, necessário se faz que tenhamos delimitado com clareza nosso objeto de estudo. O acesso não autorizado a sistemas computacionais é o objeto deste trabalho.

Em um estudo multidisciplinar, não basta, no entanto, delimitar o seu objeto, é preciso que se estabeleça também a perspectiva predominante sobre a qual aquele objeto escolhido será analisado. Assim, poderíamos analisar o acesso não autorizado a computadores do ponto de vista da Ciência da Computação, da Criminologia, da Sociologia, da Psicologia, do Direito Processual Penal e de inúmeras outras visões da ciência, mas nossa proposta aqui é uma análise predominantemente de Direito Penal.

Definidos nosso objeto de estudo e a perspectiva sobre a qual ele será trabalhado, resta-nos determinar se é possível o estudo deste objeto sobre a perspectiva escolhida.

O Direito Penal não se ocupa de qualquer conduta humana, pois só aquelas que são crimes são para ele relevantes. Assim, só será o acesso não autorizado a computadores objeto válido de estudo para o Direito Penal se for ele um crime.

Partindo de um conceito formal de crime, como conduta para a qual a lei prevê

uma sanção penal, concluiremos que, para o Direito Penal brasileiro, o acesso não autorizado a computadores não é crime, sendo, pois, objeto inválido para nosso trabalho.

Da mesma forma, se embasarmo-nos em um conceito analítico de crime, segundo o qual crime é toda conduta típica, antijurídica e culpável, o acesso não autorizado a computadores não passa de uma conduta atípica, já que não está descrita em nenhuma das centenas de tipos penais que assolam nosso sistema jurídico-penal.

Não nos limitaremos, porém, à fria leitura da norma. Busquemos então na doutrina do mestre FRAGOSO o conceito material de crime:

> *"Sob o aspecto material, é o crime um desvalor da vida social, ou seja, uma ação ou omissão que se proíbe e se procura evitar, ameaçando-a com pena, porque constitui ofensa (dano ou perigo) a um bem, ou a um valor da vida social."* (FRAGOSO, 1985. p. 147)

Diante do conceito material de crime que elege a afetação de um bem jurídico como base da ação típica[6], resta-nos definir se a conduta de quem acessa indevidamente um computador ofende ou não a um bem juridicamente tutelado.

---

[6] Para Juarez Tavares: *"O tipo, tomado sempre em sentido estrito, compõe-se, normalmente, de um núcleo, representado pela ação ou omissão e seu objeto, tendo como base a lesão a um determinado bem jurídico. A reprodução do tipo como ação indica que a norma jurídica definidora do injusto é uma norma de conduta e não uma norma meramente de reconhecimento, na terminologia proposta por Hart. Como norma de conduta, deve estar associada à determinada finalidade: a delimitação do poder de intervenção do Estado, a qual não pode ser alcançada sem um pressuposto material que lhe trace os contornos de estabilidade. Daí a necessidade de que se estabeleça, como base da ação típica, a lesão de bem jurídico."* (TAVARES, 2000. p.175-176)

REGIS PRADO ensina que:

> *"Não há delito sem que haja lesão ou perigo de lesão (princípio da lesividade ou ofensividade) a um bem jurídico determinado. Sob esta perspectiva, a tutela penal só é legítima quando socialmente necessária (princípio da necessidade), imprescindível para assegurar as condições de vida, o desenvolvimento e a paz social, tendo em conta os ditames superiores da dignidade e da liberdade da pessoa humana."* (PRADO, 2000. p.82)

A sociedade tem como valores sociais imprescindíveis para a convivência social a vida, o patrimônio, a honra, a liberdade, dentre outros[7]. Numa sociedade democrática, há que se eleger ainda a privacidade como bem jurídico fundamental e assim o fez a Constituição Federal de 1988 ao assegurar em seu art. 5º, X, que:

> *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*

Assim, a inviolabilidade das informações é decorrência natural do direito à privacidade, devendo, portanto, ser reconhecida como bem jurídico essencial para a convivência numa sociedade.

Como corolário desta afirmação, a inviolabilidade das informações automatizadas, ou seja, daquelas armazenadas e processadas em sistemas

---

[7] Nilo Batista lembra que: *"A missão do direito penal é a proteção de bens jurídicos, através da cominação, aplicação e execução da pena. Numa sociedade dividida em classes, o direito penal estará protegendo relações sociais (ou "interesses", ou "estados sociais", ou "valores") escolhidos pela classe dominante, ainda que aparentem certa universalidade, e contribuindo para a reprodução dessas relações. Efeitos sociais não declarados da pena também configuram, nessas sociedades, uma espécie de "missão secreta" do direito penal."* (BATISTA, p. 116)

computacionais, surgirá então como um novo bem jurídico a ser tutelado pelo Direito Penal, de forma a se garantir a privacidade e a integridade dos dados informáticos.

Reconhecida, pois, a existência de um bem jurídico a se proteger, tem-se que há crime sob o aspecto material, sendo que a simples omissão normativa não é suficiente para descaracterizá-lo como objeto de estudo do Direito Penal, já que este reconhece sua existência sob o aspecto material.

1.2. Informações e dados

Uma informação é toda representação que um sujeito (*res cogitans*) faz de um objeto (*res cogitata*)[8]. O nome de uma pessoa que não se quer esquecer e que procura-se a todo custo vinculá-lo à sua fisionomia. O conjunto concatenado das letras c, a, v, a, l, o, que nos remete à imagem de um animal quadrúpede em que montávamos quando criança. Uma fotografia que nos lembra de um momento feliz.

A variedade de representações criadas pela mente humana é quase infinita e abrange os cinco sentidos: uma foto, uma música, um perfume, um sabor, um beijo.

---

[8] Sobre as representações da realidade que o sujeito faz dos objetos, cf. o nosso Prolegômenos à hermenêutica jurídica. *Revista do CAAP*, Belo Horizonte, a. 3, n. 4, p. 243-263, 1998.

Evidentemente, um computador não seria capaz de armazenar ou processar tais informações, devido às suas complexidades naturais. A realidade para um computador resume-se em presença ou ausência de corrente elétrica: ligado ou desligado.

Necessário se tornou então criar uma forma de representação das informações capaz de ser processada pelos computadores.

Este tipo de representação das informações recebeu o nome de dados e baseia-se na representação dos dois estados computacionais (desligado e ligado) por dois algarismos humanos: 0 e 1. Zero representando a ausência de corrente elétrica e 1 representando sua presença.

O sistema numérico decimal é demasiadamente complexo para representar os dois estados computacionais, razão pela qual foi adotado o sistema binário que mostrou-se bem mais adequado para a representação dos dados. A correspondência entre os dois sistemas é bastante simples:

Decimal	*Binário*
0	0
1	1
2	10
3	11
4	100
5	101
6	111
7	1000

E assim sucessivamente. Note-se que a operação pode ser feita facilmente, mesmo com números grandes. Tomemos o número 345, na base decimal,

como exemplo:

$$345 / 2 = 172 \text{ resto } 1$$

$$172 / 2 = 86 \text{ resto } 0$$

$$86 / 2 = 43 \text{ resto } 0$$

$$43 / 2 = 21 \text{ resto } 1$$

$$21 / 2 = 10 \text{ resto } 1$$

$$10 / 2 = 5 \text{ resto } 0$$

$$5 / 2 = 4 \text{ resto } 1$$

$$2 / 2 = 1 \text{ resto } 0$$

Partindo do resultado final (1) e tomando todos os restos de baixo para cima chegaremos ao número 101011001 que é o correspondente binário do número decimal 345.

A operação inversa também é simples:

$$101011001 = 1x2^8 + 0x2^7 + 1x2^6 + 0x2^5 + 1x2^4 + 1x2^3 + 0x2^2 + 0x2^1 + 1x2^0$$

$$101011001 = 256 + 0 + 64 + 0 + 16 + 8 + 0 + 0 + 1 = 345$$

A representação de dados numéricos é bastante simples, porém é completamente ineficaz para representar a maioria absoluta das informações humanas comumente expressas por palavras.

A solução encontrada foi relacionar cada um dos caracteres a um número binário determinado, criando-se uma tabela:

Caracter	Código ASCII
Branco	0 000 0000
.	0 010 1110

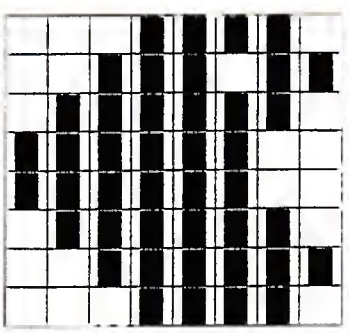
Caracter	Código ASCII
0	0 011 0000
1	0 011 0001

Caracter	Código ASCII
2	0 011 0010
3	0 011 0011
4	0 011 0100
5	0 011 0101
6	0 011 0110
7	0 011 0111
8	0 011 1000
9	0 011 1001
A	0 100 0001
B	0 100 0010
C	0 100 0011
D	0 100 0100
E	0 100 0101
F	0 100 0110
G	0 100 0111
H	0 100 1000
I	0 100 1001

Caracter	Código ASCII
J	0 100 1010
K	0 100 1011
L	0 100 1100
M	0 100 1101
N	0 100 1110
O	0 100 1111
P	0 101 0000
Q	0 101 0001
R	0 101 0010
S	0 101 0011
T	0 101 0100
U	0 101 0101
V	0 101 0110
W	0 101 0111
X	0 101 1000
Y	0 101 1001
Z	1 101 1010

Desta forma, qualquer informação humana possível de ser expressa em palavras pode ser representada por uma seqüência de zeros e uns.

As imagens também são facilmente representadas por seqüências de zeros e uns. Tomemos um exemplo simples:



00011110
00111011
01111110
11111100
11111100
01111110
00111111
00011110

Apesar da simplicidade dos exemplos, vê-se claramente que os dados nada mais são do que informações representadas de uma forma processável pelo computador.

Somente com a representação na forma de dados o computador é capaz de armazenar, processar e transmitir informações.

Para entendermos como os dados são armazenados nos computadores, imaginemos que dentro da memória[9] de um computador existam vários conjuntos de oito placas de metal cada um. Em cada um destes conjuntos seremos capazes de armazenar um caracter. Para tanto tomaremos o número binário correspondente na tabela e marcaremos com corrente elétrica a presença dos 1s constantes no número binário. O armazenamento do caracter na memória do computador estará feito.

O mesmo raciocínio pode ser aplicado à figura anterior, em que cada uma das linhas será representada por uma seqüência de oito algarismos binários.

A mesma lógica também é aplicada em disquetes (presença ou ausência de corrente eletromagnética) e CDs (reflexão ou não da luz emitida pelo laser).

Cada um dos dígitos binários 0 (desligado) e 1 (ligado) é chamado de bit (*binary digit*) e o conjunto de 8 bits foi denominado byte. Assim, cada caracter armazenado na memória de um computador equivale a 1 byte[10].

Conclui-se, pois, que os dados são informações armazenadas na forma de

---

[9] Memória - *Inform. Dispositivo em que informações podem ser registradas, conservadas, e posteriormente recuperadas; armazenador; dispositivo de armazenamento.* (FERREIRA, 1999)

10 Por estarmos trabalhando com números binários, 1 Kbyte (kilo byte) não corresponde a 1.000 bytes, mas sim a 2^{10} bytes, isto é, 1024 bytes. Da mesma forma 1 Mbyte = 2^{20} bytes = 1024x1024 bytes = 1.048.576 bytes e 1 Gbyte (giga byte) = 2^{30} bytes = 1024x1024x1024 bytes = 1.073.741.824 bytes.

bytes (ou bits, como queiram)[11].

Mais importante, no entanto, que armazenar dados, é processá-los.

O termo processo em Direito é usado para designar um conjunto de procedimentos dirigidos a um fim específico que é a solução da lide. Tais procedimentos, em geral, são estabelecidos previamente por uma lei.

No processamento de dados a idéia é a mesma. Trata-se de um conjunto de procedimentos a ser executado pelo computador, estabelecidos previamente, pela "lei das máquinas", isto é, por um programa.

Um programa é uma série de comandos muito semelhante a uma receita culinária. Tomemos um exemplo simples:

De receita:

1. *Misturar todos os ingredientes*
2. *Levar ao fogo*
3. *Aguardar dez minutos*
4. *Retirá-lo do fogo.*

De programa:

1. *Apague a tela*
2. *Escreva "Isto é um exemplo de programa"*
3. *Aguarde 30 segundos*
4. *Apague a tela*

---

[11] Para maiores detalhes sobre o funcionamento de microcomputadores cf. TORRES, Gabriel. *Hardware*: Curso Completo. 3 ed. Rio de Janeiro: Axcel Books, 1999.

5. Aguarde 30 segundos
5. Retorne à instrução nº 1

O computador, ao receber as instruções acima, as cumprirá, seguindo rigorosamente sua ordem, o que gerará na tela uma imagem da frase "Isto é um exemplo de programa". Após trinta segundos o computador apagará a tela e aguardará novos trinta segundos, quando novamente apresentará no monitor a referida frase, retomando o ciclo.

Obviamente os programas deverão também ser convertidos para uma seqüência de zeros e uns para que o computador os interprete. Este processo recebe o nome de compilação. O código na linguagem "humana" (linguagem de programação) é denominado código-fonte e o código na linguagem de máquina é denominado código-objeto.

Pelo exposto podemos concluir que:

1. Informação é qualquer representação da realidade inteligível para a mente humana;

2. Dados são informações representadas em forma apropriada para armazenamento e processamento por computadores[12];

3. Programas são séries de instruções que podem ser executadas pelo

---

[12] O *Draft Convention on Cyber-Crime* em seu artigo 1º-b assim define dados: *" 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."* <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

computador para se alcançar um resultado pretendido[13] [14].

1.3. Bem jurídico e *nomen iuris*

A boa técnica manda que se dê nome aos delitos com base no bem jurídico por ele protegido. Leia-se a lição de FRAGOSO:

> *"A classificação dos crimes na parte especial do código é questão de técnica legislativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções."* (FRAGOSO, 1983, p. 5)

Na mesma linha de raciocínio, Jair Leonardo LOPES ensina que:

> *"No CP brasileiro, os crimes são distribuídos, a partir do art. 121, por Títulos, Capítulos e Seções, de acordo com o chamado critério da objetividade jurídica, isto é, de conformidade com a natureza do bem ou objeto jurídico contra o qual se dirigiu a ação do agente. Assim, temos crimes "contra a pessoa", "crimes contra o patrimônio" e mais nove Títulos, cada qual referindo-se a um bem ou valor, considerado merecedor da reforçada proteção jurídico penal."* (LOPES, 1999, p. 113)

---

[13] O *Draft Explanatory Report* assim define programa: *"a 'computer program' is a set of instructions that can be executed by the computer to achieve the intended result."* <http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm>

[14] Cf. Lei 9.609 de 19 de fevereiro de 1998 que define em seu art. 1º: *"Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados."*

Vê-se desde já que a denominação "delitos virtuais" é completamente absurda, pois, ainda que se conceba que os delitos são praticados num mundo "virtual"[15], não haveria qualquer sentido em se falar de um bem jurídico virtual.

Restam-nos então duas opções viáveis: delitos informáticos ou computacionais.

A Ciência da Computação tem por objeto de estudo os programas de computadores, entendidos estes como qualquer série de instruções lógicas que comandem as ações da máquina. Na lição de VELLOSO:

> *"A Ciência da Computação preocupa-se com o processamento dos dados, abrangendo a arquitetura das máquinas e as respectivas engenharias de software, isto é, sua programação."* (VELLOSO, 1999, p.1)

O bem jurídico protegido no delito de acesso não autorizado a sistemas computacionais não é a inviolabilidade dos programas, mas sim da informação armazenada nos computadores, isto é, dos dados.

A ciência que tem como objeto de estudo as informações automatizadas (dados) é a Informática.

A informática é a ciência que estuda os meios para armazenar, processar e

---

[15] O termo virtual é empregado, na maioria das vezes, em Ciência da Computação, para designar uma simulação de um objetos físicos através de gráficos tridimensionais. A Internet seria então para alguns autores um universo virtual. Cf. ROHRMANN, Carlos Alberto. *O Direito Virtual:* a assinatura digital e os contratos comerciais eletrônicos. Belo Horizonte, 1999. 134f.. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Minas Gerais.

transmitir dados, isto é, para registrar, manipular e transmitir informações de forma automatizada.

> *"A origem da palavra derivou da junção dos vocábulos informação e automática, cuja criação é atribuída ao francês Philippe Dreyfus, embora, também, impute-se a autoria da expressão a Karkevitch e a Dorman."* (PIMENTEL, 2000, p. 29).

Assim, está claro que a denominação mais precisa para os delitos ora em estudo é "crimes informáticos" ou "delitos informáticos", por basear-se no bem jurídico penalmente tutelado, que é a inviolabilidade das informações automatizadas (dados).

É bom frisar que os programas também são objeto de proteção dos delitos informáticos, uma vez que também são dados.

Como vimos, para serem reconhecidos pelo computador, os programas devem estar em formato binário. Desta forma, também são informações representadas em forma apropriada para armazenamento e processamento por computadores, tendo como característica especial o fato de serem instruções que, quando executadas, geram um processamento de outros dados.

1.4. Cibernética

Há algo em comum entre leis e programas de computador. Ambos são mecanismos de controle. As leis visam ao controle da sociedade e os programas, ao controle das máquinas.

O universo está repleto de mecanismos de controle.

A natureza é regida pelas leis da Física, cujas principais manifestações são visíveis nas forças gravitacional e eletromagnética.

Os seres vivos somos controlados pelo ácido desoxirribonucléico (DNA) presente em cada uma de nossas células e muitas de nossas reações como seres humanos podem ser derivadas de uma variação da quantidade de hormônios que circulam em nosso sangue.

Nosso cérebro é controlado por impulsos eletro-químicos entre nossos neurônios. Mais que isso, como bem demonstrou Freud, não somos só um ego, mas também um id e um superego, estruturas que nos controlam a todo tempo.

No plano social, a teoria da linguagem tem demonstrado a importância do discurso como mecanismo de controle. A moral, a ética, a religião e a política exercem imensa influência sobre o comportamento de todo ser humano.

Por fim, o Direito é o meio de controle social por excelência.

A ciência que busca estabelecer uma teoria geral do controle, seja ele tanto de seres inanimados, quanto de organismos vivos, ou mesmo de máquinas é chamada de Cibernética.

Muitos autores insistem em inserir o delito de acesso não autorizado a sistemas computacionais em uma categoria que eles denominam de crimes cibernéticos. Trata-se de uma denominação completamente inadequada, baseada tão somente no uso vulgar que é dado à palavra, relacionando-a a

tudo aquilo que está vinculado às modernas tecnologias.

O objeto de estudo da Cibernética é extremamente amplo e eminentemente multidisciplinar e não tem qualquer relação com os delitos aqui estudados, extrapolando em muito os limites da presente dissertação.

O pouco que há de cibernético em nossa análise limita-se ao estudo do controle exercido pelo homem em relação a computadores e pelo ordenamento jurídico em relação àquele homem capaz de controlar tais máquinas. Nada mais.[16]

---

[16] Sobre Cibernética cf. PIMENTEL, Alexandre Freire. *O direito cibernético*: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000. 267 p. e o nosso Cibernética Penal. *Boletim do Instituto de Ciências Penais,* Belo Horizonte, a. 2, n. 16, p. 4-6, jun. 2001.

2. DA CLASSIFICAÇÃO DOS DELITOS INFORMÁTICOS

Definidos os conceitos fundamentais com os quais trabalharemos e delimitado nosso objeto de estudo, é oportuno que o classifiquemos agora – o delito de acesso não autorizado a sistemas computacionais – inserido no grupo dos delitos informáticos.

Em rigor, para que um delito seja considerado informático é necessário que o bem jurídico por ele protegido seja a inviolabilidade de dados.

A simples utilização, por parte do agente, de um computador para a execução de um delito, por si só não configuraria um crime informático, caso o bem jurídico afetado não fosse a informação automatizada.

Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando crimes informáticos os delitos em que o computador serviu como instrumento da conduta. Apesar de imprópria, esta denominação tornou-se muito popular e hoje é impossível ignorá-la.

Aos delitos em que o computador foi o instrumento para a execução do crime, mas não houve ofensa ao bem jurídico inviolabilidade da informação automatizada (dados) denominaremos Delitos Informáticos Impróprios e àqueles em que o bem jurídico afetado foi a inviolabilidade dos dados, chamaremos de Delitos Informáticos Próprios.

Aos delitos complexos em que, além da proteção da inviolabilidade dos dados, a norma visar a tutela de bem jurídico diverso, denominaremos Delitos

Informáticos Mistos.

Por fim, nos casos em que um Delito Informático Próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daquele a característica de informático, razão pela qual o denominaremos de Delito Informático Mediato ou Indireto.

2.1. Delitos Informáticos Impróprios

Delitos informáticos Impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados).

Sua popularidade é grande e, na maioria das vezes, para seu cometimento não há necessidade que o agente detenha grandes conhecimentos técnicos do uso de computadores.

Hipótese clássica de crimes informáticos impróprios são os crimes contra a honra – calúnia (art. 138 CP), difamação (art. 139 CP), injúria (art. 140 CP) – cometidos pelo simples envio de um email.

O envio de um email é uma ação absolutamente simples, que não exige conhecimento especializado e que permite não só a execução de delitos contra a honra, mas também o empreendimento dos crimes de induzimento, instigação ou auxílio ao suicídio (art. 122 CP), ameaça (art. 147 CP), violação de segredo profissional (art. 154 CP), incitação ao crime (art. 286 CP) e

apologia de crime ou criminoso (art.287 CP), entre outros.

É importante notar que em nenhum destes delitos há qualquer ofensa ao bem jurídico inviolabilidade das informações automatizadas, razão pela qual são considerados delitos informáticos impróprios.

Estes mesmos crimes também poderiam ser perfeitamente cometidos numa sala de "bate-papo" virtual (*chat*) ou através da criação de uma página na *Web*.

Ainda que de execução mais complexa que o envio de um email, a criação e publicação de uma página simples na Internet não requer conhecimentos sofisticados em computação. Seu grau de complexidade não é superior ao uso de um editor de textos ou o de uma planilha de cálculos.

Esta simplicidade, aliada à facilidade da publicação anônima das páginas criadas em servidores gratuitos, é responsável por uma expressiva quantidade de casos de publicação de fotos pornográficas de crianças na Internet, o que em nossa legislação é crime de pedofilia, previsto no art. 241 do Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069 de 13 de julho de 1990).

A Internet e os computadores são usados neste caso como instrumentos para a prática da conduta típica em sua modalidade de publicar. Aqui também temos um crime informático impróprio que em nada ofende o bem jurídico inviolabilidade de dados e, portanto, deverá ser punido com o tipo penal já existente.

Dentre os crimes informáticos impróprios previstos na legislação penal extravagante, que podem ser cometidos através da simples publicação de uma

página na Internet, há ainda os de concorrência desleal (art. 195 da Lei nº 9.279 de 14 de maio de 1996), violação de direito autoral (art. 12 da Lei nº 9.609 de 19 de fevereiro de 1998) e uma série de crimes eleitorais (art. 337 da Lei nº 4.737 de 15 de julho de 1965).

Dentre os delitos informáticos praticados na Internet, destaca-se o crime de estelionato (art. 171 do CP). As formas de execução deste crime são as mais variadas e, em geral, seu sucesso depende da confiança que a vítima deposita nos autores.

O envio de emails que solicitam à vítima o envio de pequena importância em dinheiro para os autores com a promessa de que receberão fortunas após algum tempo através de uma intricada corrente baseada numa progressão matemática é dos mais populares.

Falsas páginas de comércio eletrônico nas quais o agente efetua o pagamento mas nunca recebe o produto comprado também caracterizam o crime de estelionato na Internet.

A prostituição também é muito explorada através de páginas na Internet, nas quais há anúncios de serviços de profissionais do sexo com a exposição de fotos das mulheres. Os visitantes das páginas podem contratar os serviços *on line* o que, em tese, pode caracterizar os delitos de favorecimento da prostituição (art. 228 CP) – já que as páginas facilitam o contato com os "clientes" – ou rufianismo (art. 230 CP) – uma vez que o responsável pela página recebe comissão pelos contatos bem sucedidos.

O tráfico de drogas (art. 12 da Lei nº 6.368 de 21 de outubro de 1976) e o tráfico de armas (art. 10 da Lei nº 9.437 de 20 de fevereiro de 1997) também podem ser realizados com a simples criação de uma página na Internet, sendo que há registros de casos de indivíduos que tentaram vender substâncias entorpecentes nos populares *sites* de leilões que são acessados por milhares de pessoas diariamente[17].

Todos os casos examinados são exemplos de crimes informáticos impróprios, pois não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados).

O estudo mais acurado dos delitos informáticos impróprios excede o objetivo deste trabalho, razão pela qual passaremos à análise dos delitos informáticos próprios.

2.2. Delitos Informáticos Próprios

Delitos Informáticos Próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).

---

[17] Em 24 de setembro de 1999, três vendedores anunciaram, na página de leilões pela Internet *Ebay*, a venda de maconha em um anúncio com o título de "o melhor da Holanda" no qual constava uma foto dos agentes junto a pacotes plásticos com a droga. Sete pessoas se ofereceram para comprar o produto, em ofertas que chegaram a 10 (dez) milhões de dólares até que o anúncio fosse tirado do ar. Naquele mesmo mês foram encontrados casos de venda de órgãos humanos e de um feto na mesma página. Cf. FUOCO, Taís. Maconha é oferecida em leilões da Ebay. *Plantão Info*. Disponível em: <http://www2.uol.com.br/info/infonews/091999/24091999-2.shl>. Acesso em: 25 de setembro de 1999.

Além do delito de acesso não autorizado a sistemas computacionais – objeto deste trabalho – há ainda outras modalidades de crimes que têm como objeto a inviolabilidade dos dados informatizados e, portanto, podem ser classificados como delitos informáticos próprios.

A interferência em dados informatizados[18] é uma modalidade de crime informático próprio abrangida pelo acesso não autorizado a sistemas computacionais, porém mais específica do que ele. A hipótese procura prevenir a alteração ou destruição de dados armazenados em sistemas computacionais e sua execução implica necessariamente em um acesso não autorizado.

A lei 9.983/2000 acrescentou dois tipos penais ao Código Penal Brasileiro prevendo a hipótese da interferência em dados informatizados unicamente quando praticada por funcionário público no exercício de suas funções[19]. Em ambas as condutas previstas, não se pune a mera leitura dos dados, razão pela qual não se trata de acesso não autorizado a sistemas computacionais,

---

[18] O *Draft Convention on Cyber-Crime* em seu artigo 4º prevê tal conduta: *"Article 4 – Data interference – 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm."* <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

[19] *"Art. 313-A. Inserir ou facilitar, o funcionário 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 ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa."*

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa."

"Parágrafo único. As penas são aumentadas de 1/3 (um terço) até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado."

mas de crime especial em relação a este[20].

A interferência em sistemas computacionais[21] não se confunde com a hipótese anterior. O que se protege aqui não é a integridade dos dados em si, mas seu processamento. A inviolabilidade dos dados, neste caso, é protegida indiretamente, uma vez que perder a capacidade de processar os dados pode equivaler a perder os próprios dados.

Não há nesta hipótese um acesso aos dados armazenados no sistema. A ação do agente é no sentido de impossibilitar o funcionamento do sistema, fazendo com que as máquinas entrem em pane e parem de funcionar. A integridade dos dados permanece inviolada, porém não há mais como acessá-los, pois o sistema torna-se inoperante.

A situação mais freqüente é de ataques de recusa de serviço (*Denial of Service – DoS*)[22] [23] que são capazes de derrubar *sites* da Internet. Os prejuízos são

---

[20] *"O princípio da especialidade decorre de antiga e conhecida regra, segundo a qual a lei especial derroga a geral. De acordo com este princípio, um tipo que possui, além dos caracteres do outro, alguns mais – como acontece com os tipos qualificados em relação aos tipos básicos (homicídio criminis causa e homicídio simples, por exemplo) – ou tipos alterados em relação aos tipos não alterados (roubo e furto, por exemplo)."* (ZAFFARONI et PIERANGELI, 1999. p. 734)

[21] O *Draft Convention on Cyber-Crime* em seu artigo 5º prevê tal conduta: *"Article 5 – System interference – Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."* <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

[22] *"Essencialmente, uma atadque DoS interrompe ou nega completamente serviço a usuários legítimos, redes, sistemas e outros recursos."* (MCCLURE et al., 2000. p. 336)

[23] *"Negação de serviço, uma condição que resulta quando um usuário maliciosamente torna inoperável um servidor de informaçoes Internet, assim negando serviço de computador a*

bastante visíveis em sites de comércio eletrônico e grandes portais que perdem lucros significativos se ficarem algumas horas fora da rede. Além dos prejuízos econômicos diretos pela ausência de vendas durante o tempo em que estão fora do ar, há ainda uma conseqüência mais grave: a perda de credibilidade do consumidor com a divulgação das fragilidades do sistema.

A intererência em sistemas computacionais não está tipificada no ordenamento jurídico brasileiro.

A interceptação ilegal[24] é um crime informático próprio no qual os dados são capturados durante sua transferência de um sistema computacional para outro. O agente não obtém acesso direto ao computador da vítima, limitando-se a interceptar os dados em trânsito entre duas máquinas. Assemelha-se a uma escuta telefônica (grampo), pois os dados são lidos durante sua transmissão.

A conduta está tipificada no ordenamento jurídico pátrio na Lei nº 9.296 de 24 de julho de 1996, que em seu art. 10º dispõe:

> *"Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.*

---

usuários legítimos." (SEGURANÇA, 2000. p. 792)

[24] O *Draft Convention on Cyber-Crime* em seu artigo 3º prevê tal conduta: *"Article 3 – Illegal interception – Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."* <http://conventions.coe.int/Treaty/EN/projets/ FinalCybercrime.htm>

Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa."

Sua prática é rara se comparada ao acesso não autorizado a sistemas computacionais.

Outro importante delito informático próprio é a falsificação informática[25] que consiste na adulteração de dados de computador (seja por introdução, supressão ou simples modificação), com fins fraudulentos.

Esta hipótese é bastante ampla, mas reveste-se de especial importância na proteção dos direitos autorais sobre programas distribuídos como demonstração (*sharewares*[26]). O fraudador, nestes casos, cria pequenos programas denominados *cracks,* capazes de forjar falsos registros que fazem tais programas funcionarem sem qualquer limitação, como se tivessem sido devidamente adquiridos.

Dentre os delitos informáticos próprios, destaca-se, por fim, a criação e

---

[25] O *Draft Convention on Cyber-Crime* em seu artigo 7º prevê tal conudta: *"Article 7 – Computer-related forgery - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches."* <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

[26] *Sharewares* são programas *try before you buy* (experimente antes de comprar). Ou seja, o autor fornece uma cópia de demonstração do programa que funciona normalmente por certo período de tempo (em geral 30 dias) depois do qual o programa pára de funcionar e passa a requisitar do usuário um número de série (serial number) para voltar a funcionar normalmente. Esse número de série deve ser obtido pelo registro do programa com o conseqüente pagamento dos direitos autorais, o que em geral é feito pela própria Internet através de pagamento por cartão de crédito. (VIANNA, 1999, p. 480-481).

divulgação de programas de computadores destrutivos[27], que tem como principal representante os vírus informáticos.

A palavra vírus deriva do latim e significava originalmente "veneno". O termo acabou sendo usado pelas Ciências Biológicas para designar diminutos agentes infecciosos, visíveis apenas ao microscópio eletrônico, que se caracterizam por não ter metabolismo independente e ter capacidade de reprodução apenas no interior de células hospedeiras vivas[28].

O homem criou os vírus de computador à imagem e semelhança de seus

---

[27] O *Draft Convention on Cyber-Crime* em seu artigo 6º prevê tal conduta: *"Article 6 – Misuse of devices – 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: 1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5; 2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2)."* <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

[28] *"Quando um vírus entra em contato com uma célula hospedeira, acopla-se a ela através da cauda e perfura a membrana celular por meio de ação enzimática. Então, o ácido nucléico viral é injetado no interior da bactéria, passando a interferir no metabolismo bacteriano de maneira a comandar a síntese de novos ácidos nucléicos virais, à custa da energia e dos componentes químicos da célula vítima. Paralelamente, e ainda utilizando a célula hospedeira como fonte de energia e de matéria-prima, o ácido nucléico do vírus comanda a síntese de várias outras moléculas que, ao se juntarem, de maneira ordenada, definem a formação de novos vírus (...). Uma vez formadas, as novas unidades virais promovem a ruptura da membrana bacteriana (lise) e os novos vírus liberados podem infectar outra célula, recomeçando um novo ciclo."* (PAULINO, 1990. p.19-20)

homônimos biológicos. Os vírus de computador são programas que infectam outros programas, podendo causar variados danos aos dados armazenados no sistema e se reproduzindo a partir do hospedeiro[29]. São programas extremamente pequenos, escritos geralmente em Assembly, C ou Pascal, capazes de se reproduzir através da contaminação de disquetes ou, modernamente, por meio de emails.

Na legislação brasileira não há um tipo penal específico visando à repressão dos vírus informáticos, mas é perfeitamente possível a punição por crime de dano (art. 163 do CP) quando a conduta destruir, inutilizar ou deteriorar os dados armazenados no sistema computacional.

Alguns juristas nacionais entendem que os dados não podem ser considerados coisa e, portanto, não estariam protegidos pela norma. Ora, se não são coisas são o quê?

Coisa é *tudo aquilo que existe ou pode existir* (FERREIRA, 1999). Se os dados existem, são coisas.

Não se pode esquecer que a gravação dos dados tanto em disquetes como em discos rígidos é feita por meio magnético, da mesma forma que uma gravação realizada numa fita K7 ou VHS. Se se admitir que a destruição dos dados

---

[29] Nunca é demais ressaltar que os vírus informáticos nenhum mal podem causar ao organismo humano, pois nada mais são do que programas de computador destrutivos. Esta observação, certamente, é demasiadamente óbvia para a maioria dos leitores, mas já se propôs ação reclamatória trabalhista em que se pretendia receber adicional de insalubridade pelo fato do reclamante trabalhar com computadores infectados por vírus. (Cf. Processo nº. 00950/95 – 14ª Junta de Conciliação e Julgamento de Belo Horizonte)

armazenados num sistema computacional não tipifica o crime de dano, impossível também será a condenação por dano pela inutilização de uma fita K7 ou VHS por exposição a meio magnético (um ímã, por exemplo).

Apesar de ser perfeitamente aplicável a condenação por dano causado por vírus de computador, melhor seria que houvesse lei específica prevendo a criação e divulgação dos vírus como crime de perigo concreto[30].

Ressalte-se, no entanto, que a tipificação da criação e divulgação de vírus deve prever como elemento subjetivo do tipo o dolo específico de causar dano, pois caso contrário estar-se-ia impedindo que programadores bem intencionados criassem vírus para estudo, até mesmo como forma de criar antídotos contra outros já existentes.

2.3. Delitos Informáticos Mistos

Delitos Informáticos Mistos são crimes complexos[31] em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza

---

[30] *"Com vista ao bem jurídico protegido, é que se fala em crimes de dano e em crimes de perigo. Os primeiros causam lesão efetiva, os últimos conduzem uma potencialidade de lesão, realizável ou não, em concreto, que o legislador deseja cortar no nascedouro. Estes – os de perigo – se subdividem em crimes de perigo concreto e em crimes de perigo abstrato ou presumido. Nos de perigo concreto a realização do tipo exige constatação, caso a caso, de perigo real, palpável mensurável. Nos de perigo abstrato, ao contrário, dispensa-se essa constatação, por se tratar de perigo presumido de lesão."* (TOLEDO, 1994. p. 143).

[31] *"Crimes simples e complexos: simples é o que se identifica com um só tipo legal; complexo, o que representa a fusão unitária de mais de um tipo (ex.: roubo, estupro)."* (HUNGRIA, 1958. p. 53).

diversa.

São delitos derivados[32] do acesso não autorizado a sistemas computacionais que ganharam *status* de delitos *sui generis* dada à importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.

No ordenamento jurídico brasileiro, paradoxalmente, um delito informático derivado do acesso não autorizado a sistemas computacionais já foi tipificado, enquanto que o delito fundamental ainda aguarda regulamentação.

Trata-se do acesso não autorizado a sistemas computacionais do sistema eleitoral que surgiu como tipo penal no ordenamento jurídico nacional com a Lei 9.100/95 que em seu art. 67, VII, assim o tipificou:

> *"obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos."*

A pena prevista foi de 1 (um) a 2 (dois) anos de reclusão e multa.

Dois anos depois, a Lei 9.504/97, em seu art. 72, I, assim dispôs sobre a

---

[32] *"Classificam-se os tipos em básicos ou fundamentais e derivados, compreendendo estes as figuras de crimes qualificados e privilegiados. Os tipos básicos constituem a espinha dorsal do sistema na parte especial (Mazger). As derivações são formuladas tendo-se em vista que apresentam, em relação ao tipo básico, diverso merecimento de pena, pela ocorrência de circunstâncias que agravam ou atenuam, particularmente, a antijuridicidade do fato ou a culpabilidade do agente, na perspectiva de determinada figura do delito. Em alguns casos, limita-se o legislador a introduzir, no mesmo dispositivo de lei, hipóteses agravadas ou atenuadas dos tipos básicos, formando, assim, crimes qualificados ou privilegiados. (...) Em outros casos, no entanto, temos a formação, como novos elementos que tornam o crime mais ou menos grave, de uma nova figura de delito. Surge, então, um delictum sui generis, que constitui, para todos os efeitos, um tipo autônomo de crime, excluindo a aplicação do tipo básico."* (FRAGOSO, 1985. p. 160-161)

matéria:

> *"obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos."*

A redação do tipo é praticamente idêntica à anterior, mas a pena foi elevada para de 5 (cinco) a 10 (dez) anos de reclusão. Não houve, no entanto, revogação total do dispositivo anterior, pois, se o delito consumado foi inteiramente regulado pela nova lei, o mesmo não ocorreu com o crime tentado.

Assim, encontra-se parcialmente em vigor o art. 67, VII, da Lei 9.100/95, disciplinando exclusivamente os casos de tentativa, pois a aplicação do parágrafo único do art. 14 do CP, por sua própria disposição, é meramente subsidiária e este só pode ser utilizado quando não há nenhuma regulamentação da matéria.

Frise-se ainda que o art. 107 da Lei 9.504/97 enumera taxativamente os dispositivos por esta revogados e em seu rol não há qualquer menção ao art. 67, VII, da Lei 9.100/95.

As ameaçadoras penas cominadas a este crime eleitoral só demonstram uma triste realidade: a preocupação demasiada do legislador em impor penas altas e sua completa alienação quanto à efetividade da norma.

Ao contrário do que crê grande parte da população, a urna eletrônica usada nas eleições brasileiras é completamente vulnerável a acessos não autorizados e, muito dificilmente, um delito como este poderia ser apurado.

É que o código-fonte do programa usado pela urna não é aberto[33], o que equivale a dizer que toda a legitimidade das eleições brasileiras é garantida pelo seleto grupo de programadores que desenvolvem o *software*.

A política de segurança do TSE (Tribunal Superior Eleitoral) parece basear-se unicamente no sigilo dos fontes. Tal opção é profundamente temerosa, pois um único dos programadores que se corrompesse poderia colocar em risco a legitimidade de uma eleição inteira.

Não sendo os códigos públicos, não há como os partidos terem certeza de que o programa que está sendo usado pela urna no dia das eleições efetivamente cumpra sua função de coletar e totalizar os votos sem nenhuma alteração, pois poderiam ser perfeitamente modificados para garantir a vitória de um determinado candidato.

O TSE argumenta que a publicidade do código fonte facilitaria a fraude, pois qualquer progamador estaria apto a tentar manipular as eleições. Trata-se evidentemente de um sofisma, pois desconsidera a intensa fiscalização que passaria a ser exercida pelos partidos políticos.

Além do mais, a legitimidade das eleições brasileiras não deveria fundamentar-

---

[33] Isto significa dizer que os desenvolvedores não tornaram público o código-fonte, só fornecendo o código-objeto. Cynthia Machado ensina que: *"O software é um conjunto ordenado de instruções dadas à máquina, que faz com ela realize determinada tarefa. Para isso, tais instruções são escritas, como um texto, sendo denominadas código-fonte. Posteriormente, essas instruçoes são convertidas na linguagem do computador, em um processo de compilação, resultando no software que é distribuído comercialmente. É importante observar que a distribuição comercial não disponibiliza o código-fonte, mas apenas os arquivos compilados, que só podem ser entendidos pelo computador."* (MACHADO, 2001, p. 6)

se no sigilo dos códigos-fontes, mas sim, em modernas técnicas de criptografia que garantiriam um grau de segurança que tornaria completamente dispensável o segredo do código.

2.4. Delito Informático Mediato ou Indireto

Delito Informático Mediato ou Indireto é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

Se alguém acessa sem autorização o sistema computacional de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o acesso não autorizado a sistemas computacionais e o furto; o primeiro, crime informático, o segundo, patrimonial.

O acesso não autorizado será executado como delito-meio para se poder executar o delito-fim que consiste na subtração da coisa alheia móvel. Desta forma, o agente só será punido pelo furto, aplicando-se ao caso o princípio da consunção.

> *"Em função do princípio da consunção, um tipo descarta outro porque consome ou exaure o seu conteúdo proibitivo, isto é, porque há um fechamento material."* (ZAFFARONI et PIERANGELI, 1999. p. 735)

O crime-fim será classificado como informático mediato ou indireto quando, pela aplicação do principio da consunção, um crime-meio informático não for

punido em razão da sua consumação.

O delito informático mediato não se confunde com o delito informático impróprio, pois aqui há lesão ao bem jurídico inviolabilidade dos dados informáticos, ainda que esta ofensa não seja punida pela aplicação do princípio da consunção.

Não se confunde também com o delito informático misto, pois aqui há dois tipos penais distintos, em que cada um protege um bem jurídico.

Pode-se citar ainda como exemplo de delito informático mediato o acesso indevido a um banco de dados de uma empresa de comércio eletrônico para a aquisição dos números de cartões de crédito dos clientes.

O uso posterior destes números de cartões de crédito para a realização de compras na Internet constituiria um estelionato. Aplicar-se-ia o princípio da consunção e o agente seria punido tão somente pelo delito patrimonial.

3. DOS ELEMENTOS CRIMINOLÓGICOS

Classificados os delitos informáticos, buscaremos neste capítulo analisar do ponto de vista da Criminologia o comportamento de seus autores.

3.1. As motivações

Temos como axioma que a Criminologia não é a ciência que tem como objeto o crime, mas sim, os crimes. Não cremos que os fatores que movam um homicida sejam os mesmos que impulsionam um estuprador. Buscar semelhanças em seus comportamentos sob o pretexto de que ambos são criminosos não nos parece ser o melhor método para se trabalhar a Criminologia. Evidentemente pode-se encontrar algumas semelhanças em seus comportamentos, mas, certamente, as diferenças serão maioria.

As teorias subculturais e as teorias da aprendizagem social (*Social Learning*) parecem explicar bem parte das motivações dos criminosos informáticos.

SUTHERLAND elaborou uma teoria conhecida como Teoria das Associações Diferenciais para explicar os crimes de colarinho branco na qual analisou as formas de aprendizagem do comportamento criminoso.

> *"A hipótese aqui sugerida em substituição das teorias convencionais, é que a delinqüência de colarinho branco, propriamente como qualquer outra forma de delinqüência sistemática, é aprendida; é aprendida em associação direta ou indireta com os que já praticaram um comportamento criminoso, e aqueles que aprendem este*

> *comportamento criminoso não tem contatos freqüentes e estreitos com o comportamento conforme a lei. O fato de que uma pessoa torne-se ou não um criminoso é determinado, em larga medida, pelo grau relativo de freqüência e de intensidade de suas relações com os dois tipos de comportamento. Isto pode ser chamado de processo de associação diferencial."*(SUTHERLAND, E. H. White-Collar Criminality in *American Sociological Review*, V, p. 11, 1940. *apud* BARATTA, 1999)

Mais do que em qualquer outro tipo de atividade criminosa, um crime informático antes de ser executado deve ser aprendido. Crimes clássicos como homicídio, furto e estupro não exigem qualquer tipo de conhecimento para serem cometidos, o que decididamente não é o caso dos crimes informáticos que, por sua própria natureza, exigem um aprofundado estudo de técnicas que permitam o domínio do computador para utilizá-lo na conduta criminosa.

Por mais que uma significativa parcela dos piratas afirme ser autodidata, não restam dúvidas de que grande parte das técnicas de invasão de computadores são ensinadas por piratas mais experientes na própria Internet. Uma simples busca em mecanismos de procura com o termo *hacker* gerará centenas de páginas contendo uma série de técnicas que ensinam os primeiros passos para se tornar um criminoso informático.

Ressalte-se que não se trata de um mero aprendizado técnico. Ocorre que na busca pelo conhecimento técnico o indivíduo acaba se influenciando pela subcultura *cyberpunk* na qual o reconhecimento de sua capacidade intelectual está diretamente relacionado às suas proezas ilegais. A invasão de páginas importantes como as do FBI e da NASA garantem a seus autores grande prestígio. As pichações digitais são sinais de poder intelectual dentro da

subcultura *cracker* e geram respeito e fama a seus autores.

Por outro lado, aqueles que não agem como *crackers* são considerados incompetentes e ignorantes e acabam sendo excluídos da comunidade *cyberpunk*. A idéia dominante no meio é de que conhecimento gera conhecimento e a maioria deles não parece estar disposta a compartilhar informações com quem não possa oferecer nada em troca.

Desta forma, o indivíduo acaba sendo induzido à prática de crimes digitais para obter respeito dentro da subcultura, o que lhe garantirá mais informações e conseqüentemente maiores proezas e mais respeito.

Os meios de comunicação contribuíram bastante para a formação de um estereótipo romântico dos piratas, descrevendo-os como gênios de computadores capazes de disparar bombas atômicas com um *notebook* conectado a um celular. Esta imagem de poder estimula a ação de muitos jovens ainda em processo de formação social.

Assim se dá a transformação em um criminoso digital do indivíduo curioso que busca na Internet soluções para problemas técnicos. Mas é importante também procurar definir quais indivíduos estão mais propensos a se tornarem piratas.

COHEN analisa as razões de existência da subcultura e do seu conteúdo específico. A estrutura social induz nos adolescentes da classe operária a incapacidade de se adaptar aos *standards* da cultura oficial e, além disso, faz surgir neles problemas de status e de autoconsideração.

> *"A teoria das subculturas criminais nega que o delito possa ser considerado como expressão de uma atitude*

> *contrária aos valores e às normas sociais gerais, e afirma existirem valores e normas específicos dos diversos grupos sociais (subcultura).*" (BARATTA, 1999. p.73.)

A teoria de COHEN de que a marginalização de um grupo acaba gerando a criminalidade adapta-se perfeitamente à realidade da maioria dos piratas.

Os motivos que levam à marginalização dos piratas em seu meio não são de ordem econômica, mas intelectual. A maioria dos criminosos virtuais possui uma inteligência bem acima da média e, quando crianças, acabam sendo marginalizados pelos colegas, que os rotulam de "caxias" ou "nerds".

Não se trata, no entanto, de crianças aplicadas ou estudiosas, muito pelo contrário. A facilidade com que resolvem os trabalhos escolares acaba tornando-se um fator de desestímulo. Os professores os consideram alunos problemáticos e rebeldes.

Esta dificuldade de adaptação social quando crianças acaba sendo compensada na adolescência, ao tomarem contato com os computadores.

No mundo virtual eles são populares e admirados por seus feitos. Na Internet eles não são marginalizados, muito pelo contrário, eles marginalizam aqueles sem o conhecimento necessário para ser um *cracker*.

O sistema de valores do pirata torna-se, pois, totalmente diverso do sistema de valores sociais predominante. Passam a respeitar códigos de ética próprios criados dentro da subcultura, onde o conhecimento é a moeda de maior valor (daí muitos deles desprezarem os que agem com fins econômicos).

Há ainda que se analisar as técnicas de neutralização descritas por SYKES e

MATZA em seu trabalho *Techniques of Neutralization*, (*apud* BARATTA, 1999. p. 78.) que podem perfeitamente ser aplicadas aos piratas:

a) exclusão da própria responsabilidade – grande parte dos *crackers* justifica suas atitudes como sendo algo incontrolável; um vício. Efetivamente há vários casos de piratas que mesmo após sofrerem condenações penais nos Estados Unidos, voltaram a invadir sistemas compulsivamente.

b) negação de ilicitude – o pirata interpreta sua conduta como somente proibida, mas não imoral ou danosa. A invasão de um computador sem a alteração ou a exclusão dos dados lá armazenados é considerada por muitos piratas uma prática perfeitamente moral, já que não provoca qualquer prejuízo à vítima.

c) negação de vitimização – argumento clássico dos *crackers* é o de que a vítima mereceu a invasão, pois não tomou as medidas de segurança necessárias para evitá-la. Para a maioria dos piratas, na Internet vale a lei do mais inteligente e se um computador foi invadido é porque o responsável por ele é um incompetente que não se preveniu adequadamente. Aliás, a justificativa dada pelos programadores de vírus para a sua conduta é de que computadores não devem ser usados por pessoas sem formação adequada e, portanto, os vírus seriam uma forma de extinguir usuários sem os conhecimentos técnicos que eles julgam imprescindíveis para operar um computador.

d) condenação dos que condenam – os piratas julgam viver numa sociedade hipócrita na qual as pessoas que os condenam cometem ações muito mais

graves do que as deles.

e) apelo a instâncias superiores – a maioria dos *crackers* segue um código de ética que varia de acordo com o grupo a que pertence[34].

3.2. Sistematização criminológica

O criminólogo Marc ROGERS[35], da Universidade de Manitoba, Canadá, classifica os *hackers*[36] em sete diferentes categorias (que não necessariamente se excluem): *newbie/tool kit* (NT), *cyberpunks* (CP), *internals* (IT), *coders* (CD), *old guard hackers* (OG), *professional criminals* (PC), and *cyber-terrorists* (CT). Tais categorias estão numa ordem hierárquica que varia do menor nível técnico

---

[34] Eis um exemplo de código *cracker* que pode ser encontrado na Internet:

"My Code of Ethics - All true hackers have thier own set of ethics, a sort of rules that he/she goes by when hacking. The ethics of a real hacker are much different from that of a lamer or virus spreader. All a lamer cares about is getting warez and forgetting credit where credit is due. All a virus spreader wants to do is spread viruses and delete files. People such as this are to be considered scum, and they give the true hacker a bad name. No skill or artistic expression is required to do what they do. The true hacker goes by his ethical code, respecting the computers he works on and hacks. Here is my code of ethics:

Above all else, respect knowlege & freedom of information; notify system administrators about any security breaches you encounter; do not profit unfairly from a hack;·do not distribute or collect pirated software; never take stupid risks - know your own abilities;·always be willing to freely share and teach your gained information and methods; never hack a system to steal money; never give access to someone who might do damage; never intentionally delete or damage a file on a computer you hack; respect the machine you hack, and treat it like you'd treat your own system."

SCORPIO (2001) <http://www.attrition.org/~modify/texts/ethics/my.code.of.ethics.html>.

[35] Cf. ROGERS, Marc. *A new hacker taxonomy.* Disponível em: <http://www.escape.ca/~mkr/hacker_doc.pdf>.

[36] Utilizaremos o termo *hackers* aqui por ter sido usado por ROGERS em sua classificação.

(NT) ao maior (OG-CT).

A categoria NT é formada por *hackers* que possuem técnicas limitadas. Utilizam-se de programas prontos que obtêm na própria Internet. A categoria CP é composta por *hackers* que geralmente possuem bons conhecimentos de computação e são capazes de desenvolver seus próprios programas, conhecendo bem os sistemas que atacam. Eles praticam condutas mal-intencionadas como alterar páginas e enviar seqüências de *e-mails* com o fim de esgotar a capacidade da caixa-postal da vítima. Muitos estão envolvidos em fraudes com cartões de crédito e telefonia.

A categoria IT é formada por empregados descontentes ou ex-funcionários que se aproveitam dos conhecimentos técnicos adquiridos na empresa para atacá-las como forma de retaliação. Segundo ROGERS este grupo é responsável por 70% de toda atividade criminosa envolvendo computadores.

O grupo OG não possui intenções criminosas, salvo o enorme desrespeito com que encaram a privacidade alheia. Esforçam-se para adquirirem conhecimentos e consubstanciam a ideologia da primeira geração de *hackers*.

As categorias dos PC e CT são as mais perigosas. São criminosos profissionais e ex-agentes da inteligência que atacam por dinheiro. São especialistas em espionagem corporativa e freqüentemente bem treinados. A categoria se expandiu com a dissolução das agências de inteligência do leste europeu.

A classificação de ROGERS peca por misturar critérios de ordem objetiva (nível

técnico) com elementos subjetivos (motivação, intenção).

Acreditamos não haver sentido algum em classificar os *hackers* de acordo com seu nível técnico. Poderíamos listar três categorias: neófitos, experientes e veteranos, mas esta classificação poderia ser feita em cinco, sete ou em até dez categorias, o que não haveria sentido algum.

Optamos por uma sistematização de ordem objetiva dos piratas levando em conta, tão somente, seu *modus operandi*:

1) *CRACKERS* DE SISTEMAS – piratas que invadem computadores ligados em rede.

2) *CRACKERS* DE PROGRAMAS – piratas que quebram proteções de *software* cedidos a título de demonstração para usá-los por tempo indeterminado, como se fossem cópias legítimas.

3) *PHREAKERS* – piratas especialistas em telefonia móvel ou fixa.

4) DESENVOLVEDORES DE VÍRUS, *WORMS* e *TROJANS* – programadores que criam pequenos *softwares* que causam algum dano ao usuário.

5) PIRATAS DE PROGRAMAS– indivíduos que clonam programas, fraudando direitos autorais.

6) DISTRIBUIDORES DE *WAREZ* – *webmasters* que disponibilizam em suas páginas *softwares* sem autorização dos detentores dos direitos autorais.

Vista esta classificação objetiva, é necessário agora estudarmos mais

detidamente os *crackers* de servidores (espécie do gênero pirata), pois são eles os autores do delito de acesso não autorizado a sistemas computacionais, objeto deste trabalho. Para tanto, faremos uma classificação de ordem subjetiva dividindo-os de acordo com suas motivações:

1) CURIOSOS – agem por curiosidade e para aprender novas técnicas. Não causam danos materiais à vítima. Lêem os dados armazenados, mas não modificam nem apagam nada. Muitos seguem códigos de ética próprios ou de um grupo ao qual são filiados.

2) PICHADORES DIGITAIS[37] – agem principalmente com o objetivo de serem reconhecidos. Desejam tornar-se famosos no universo *cyberpunk* e para tanto alteram páginas da Internet, num comportamento muito semelhante aos pichadores de muro, deixando sempre assinado seus pseudônimos. Alguns deixam mensagens de conteúdo político, o que não deve ser confundido com o ciberterrorismo.

3) REVANCHISTA – funcionário ou ex-funcionário de uma empresa que decide sabotá-la com objetivo claro de vingança. Geralmente trabalharam no setor de informática da empresa, o que facilita enormemente a sua ação, já que estão bem informados das fragilidades do sistema.

4) VÂNDALOS – agem pelo simples prazer de causar danos à vítima. Este

---

[37] As telas com os conteúdos das "pichações digitais" de maior repercussão na Internet brasileira são encontradas no Anexo C.

dano pode consistir na simples queda do servidor (deixando a máquina momentaneamente desconectada da Internet) ou até mesmo a destruição total dos dados armazenados.

5) ESPIÕES – agem para adquirirem informações confidenciais armazenadas no computador da vítima. Os dados podem ter conteúdo comercial (uma fórmula de um produto químico), político (*emails* entre consulados) ou militar (programas militares).

6) CIBERTERRORISTAS – são terroristas digitais. Suas motivações são em geral políticas e suas armas são muitas, desde o furto de informações confidenciais até a queda do sistema telefônico local ou outras ações do gênero.

7) LADRÕES – têm objetivos financeiros claros e em regra atacam bancos com a finalidade de desviar dinheiro para suas contas.

8) ESTELIONATÁRIOS – também com objetivos financeiros; em geral, procuram adquirir números de cartões de créditos armazenados em grandes *sites* comerciais.

Evidentemente, nada impede que um mesmo *cracker* de servidor aja com duas ou mais motivações, ou que, com o passar do tempo, mude de motivações. Aliás, possivelmente é o que ocorre com maior freqüência.

4. DO DIREITO ESTRANGEIRO[38]

O delito informático próprio de acesso não autorizado a sistemas computacionais ainda não se encontra tipificado na legislação brasileira. Há alguns projetos de leis nacionais que visam a tipificação do delito, destacando-se dentre eles o Projeto de Lei nº 84 de 1999[39] de autoria do Deputado Luiz Piauhylino.

Nos Estados Unidos e na maior parte da Europa, no entanto, a criminalização desta conduta já é fato há anos e continua, até hoje, sendo objeto de profunda discussão nos meios jurídicos internacionais.

A primeira proposta de tipificação do acesso não autorizado a computadores no mundo deu-se em 1977, nos EUA (Estados Unidos da América), quando o Senador Ribikoff apresentou ao Congresso daquele país um projeto de lei que

---

[38] A íntegra das legislações estrangeiras e dos projetos comentados neste capítulo pode ser encontrada nos Anexos A e B respectivamente, bem como no Anexo D (CD-ROM).

[39] Acesso indevido ou não autorizado
Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.
Pena: detenção, de seis meses a um ano e multa.
Parágrafo primeiro. Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.
Parágrafo segundo. Se o crime é cometido:
I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de um a dois anos e multa.
<http://www.camara.gov.br/LuizPiauhylino/textopl84.doc>

visava disciplinar crimes informáticos. Seu projeto nunca foi aprovado, mas sua proposta gerou discussões na comunidade jurídica internacional.

Só em 1984 os EUA adotaram uma legislação que visava coibir os crimes informáticos que foi revista dois anos mais tarde, dando origem ao famoso *Computer Fraud and Abuse Act* de 1986.

Posteriormente, em 1988, ocorreu nos EUA o caso USA vs. Robert Tappan Morris que teve repercussão nacional e acabou gerando o precedente jurisprudencial adotado pelas cortes americanas na aplicação do *Computer Fraud and Abuse Act.*

O estudante de computação da Universidade de Cornell, Robert Morris, foi condenado a três anos de prisão[40] por lançar na Internet um pequeno programa de computador conhecido como *worm* (verme) que buscava máquinas vulneráveis na rede e as infectava com uma cópia de si mesmo. O programa espalhou-se rapidamente e provocou um sobrecarregamento até então jamais visto na rede, despertando na sociedade americana uma grande preocupação quanto à segurança dos sistemas computacionais.

Em 1990, Morris apelou da sentença e teve seu apelo rejeitado, pois o Tribunal entendeu que a lei não exigia o fim especial de agir de "causar dano" para a caracterização do crime, bastando o dolo genérico do agente de acessar sem

---

[40] Que cumpriu em liberdade condicional, por ser primário e possuir bons antecedentes. (Cf. GEHRINGER et LONDON, 2001. p. 53)

autorização o sistema computacional para que ocorresse a tipicidade da conduta.

Naquela ocasião decidiu-se ainda que quaisquer computadores situados em estados diferentes e ligados entre si em rede deveriam ser considerados de interesse federal e, portanto, julgados com base no *Computer Fraud and Abuse Act*. O conceito evoluiu e hoje são considerados de interesse federal os computadores utilizados no comércio interestadual.

Por esta interpretação, qualquer computador conectado à Internet pode ser considerado como de interesse federal, permitindo que os crimes praticados na Grande Rede sejam julgados na jurisdição federal. Na prática, a maioria dos casos de crimes informáticos nos Estados Unidos são julgados pela jurisdição federal, principalmente por uma questão prática, uma vez que os órgãos estaduais em sua grande maioria não estão preparados tecnicamente para coibir os delitos informáticos. Além do mais, a grande maioria das legislações estaduais são baseadas no *Computer Fraud and Abuse Act* e disciplinam a matéria de forma muito semelhante.

Atualmente os casos de condenações por acessos não autorizados a computadores nos EUA são bastante freqüentes e a mídia norte-americana dá grande destaque aos fatos, como nos casos das condenações dos *crackers* Kevin Poulsen[41] e Kevin Mitnick[42].

---

[41] Kevin Lee Poulsen, conhecido no meio *hacker* como Watchman, envolveu-se cedo com o

Na Europa, o acesso não autorizado a sistemas computacionais também é objeto de tipificação em inúmeras legislações.

Na Itália[43], a Lei nº 547 de 23 de dezembro de 1993 introduziu no Código Penal o acesso abusivo a um sistema informático ou telemático como conduta típica.

---

acesso não autorizado a computadores. Foi indiciado aos 17 anos, e só não foi preso por ser menor de idade. Trabalhou em projetos militares na SRI International, e depois na Sun Microsystems, voltando aos poucos ao acesso não autorizado. Invadiu a Pac Bell (companhia telefônica), descobriu grampos não autorizados (inclusive de consulados), criou um sistema de facilitação de prostituição via telefone e ganhou diversos concursos de rádio com prêmios como viagens ao Havaí e um Porsche, manipulando ligações telefônicas. Indiciado em 1989, tornou-se fugitivo, sendo preso em 1991. Foi o primeiro hacker acusado de espionagem (além de fraude de computadores, interceptação de comunicações eletrônicas, fraude de correio, lavagem de dinheiro e obstrução da justiça). Um acordo entre a Promotoria e a defesa pôs fim à acusação de espionagem. Mesmo assim, Poulsen ficou preso até 1996, cumprindo ainda mais três anos de condicional sem contato com computadores, o que impossibilitava que ele arranjasse emprego e pudesse restituir os valores obtidos com as fraudes em programas de rádio. Sobre a vida de Kevin Poulsen cf. LITTMAN, Jonathan. *Watchman*: a vida excêntrica e os crimes do serial hacker Kevin Poulsen. Rio de Janeiro: Record, 1998.

[42] Kevin David Mitnick, o Condor, é o hacker mais famoso do mundo e se destacou em técnicas simples, mas de grande efeito, como a "engenharia social", para obter acesso não autorizado a diversos computadores, fosse para obter informações, fosse para passar trotes em seus amigos e inimigos. Foi preso pela primeira vez nos anos 80, chegando a passar vários meses na solitária por sua suposta periculosidade. Após ser solto, continuou praticando acessos não autorizados e, indiciado, manteve-se fugitivo por muitos anos. Foi preso em 1995 em uma controvertida manobra do FBI que incluiu um jornalista do New York Times, caçadores de recompensas e um outro hacker – Tsutomu Shimomura – que considerava questão de honra prender Mitnick por acreditar que ele invadira seu computador (fato negado por Mitnick). Também se supõe que Mitnick tenha invadido o Pentágono e inspirado o filme "Jogos de Guerra", mas ele sempre negou tal versão, afirmando que nunca se envolveu em questões militares. Fato interessante a respeito dele é que não há provas de que tenha se utilizado de seus conhecimentos técnicos e acessos para obter vantagem pessoal, além de, durante todo o período em que foi fugitivo, ter trabalhado normalmente, com identidade falsa, como uma pessoa comum. Mitnick ficou preso de 1995 a 2000, e seu processo judicial foi criticado pela demora injustificada do julgamento, mesmo porque aguardou o julgamento preso. Houve críticas ainda quanto ao cerceamento de defesa, já que Mitnick não podia acessar a biblioteca da prisão, foi levado a "solitária" sem razões concretas e só teve direito a um advogado após quatro meses de sua prisão, pois a justiça americana não aceitava pagar um defensor para representá-lo nos tribunais. Sobre a vida de Kevin Mitnick cf. LITTMAN, Jonathan. *O jogo do fugitivo*: em linha direta com Kevin Mitnick. Rio de Janeiro: Rocco, 1996.

[43] *"Art. 615 ter. Accesso abusivo ad un sistema informatico o telematico - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni."*
<http://www.studiocelentano.it/cp/codicepenale002a.htm>

De acordo com este dispositivo, aquele que abusivamente penetra em um sistema informático ou telemático protegido por meios de segurança ou permanece nele contra a vontade expressa ou tácita de quem tem o direito de excluí-lo está sujeito a prisão não superior a 3 (três) anos.

O delito será qualificado e terá penas de 1 (um) a 5 (cinco) anos quando cometido por funcionário público, encarregado de serviço público, investigador particular, administrador de sistema ou com abuso de poder e violação de dever inerente à função ou serviço. Também será qualificado quando do fato derivar a destruição ou dano ao sistema ou interrupção total ou parcial de seu funcionamento, bem como na destruição ou na perda dos dados, das informações e dos programas nele contidos.

A lei italiana prevê ainda que o delito será qualificado quando praticado mediante violência à coisa ou à pessoa ou quando o agente estiver armado. A hipótese parece limitar-se aos acessos não autorizados locais, isto é, àqueles em que o agente tem contato físico com o computador.

Os computadores de interesse militar e todos aqueles considerados de interesse público também foram especialmente protegidos pela norma italiana.

Na França[44], o fato de acessar ou se manter, fraudulentamente, no todo ou em

---

[44] *"Article 323-1. Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100.000 F d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende."*
<http://fabrice.gauthier.free.fr/fabrice/fichiers/pdf/cppdf.zip>

parte em um sistema de tratamento automático de dados é punido com até um ano de prisão e multa de 100.000 F (cem mil francos franceses).

O delito será qualificado quando resultar na supressão ou na modificação de dados contidos no sistema, ou na alteração de seu funcionalmento, hipótese na qual a pena será de até dois anos de prisão e multa de 200.000 F (duzentos mil francos franceses).

A punição da tentativa é prevista expressamente no art. 323-7 do Código Penal Francês.

As legislações penais italiana e francesa tipificam não só o acesso não autorizado, mas também o excesso do acesso autorizado.

A lei francesa prevê ainda expressamente a hipótese do acesso parcial, pois muita vez, o agente não consegue um acesso a todos os diretórios do sistema.

Na Alemanha[45], a conduta típica é obter, para si ou para outrem, sem autorização, dados para si não destinados e protegidos contra acesso não

---

[45] *"§ 202a Ausspähen von Daten - (1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, ma- gnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."* <http://www.datenschutz-berlin.de/recht/de/rv/szprecht/stgb/index.htm>.

O artigo foi transcrito *ipsis verbis* do Código Penal Alemão, mas nossos comentários basearam-se na seguinte tradução não oficial para o inglês: *"Section 202a Data Espionage - (1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine. (2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner."* <http://www.bmj.de/publik/e_stgb.pdf >

autorizado. A pena prevista é de até 3 (três) de prisão.

Havendo alteração dos dados, o agente será punido nos termos do § 303a com até 2 (dois) anos de prisão, o que parece ser uma grande contradição da lei penal alemã, pois, havendo modificação nos dados, a pena é menor do que a simples cópia dos dados, que mantém os originais intactos.

Outra crítica a ser feita à lei germânica é quanto à lacuna por ela deixada em relação à proteção dos programas armazenados em computadores. É que, muita vez, o acesso se dá visando tão somente à obtenção de *softwares*, como em inúmeros casos de subtração de programas militares de uso exclusivo das forças armadas.

A lei alemã refere-se exclusivamente à proteção de dados, o que, em uma interpretação literal da norma, poderia levar à absolvição do agente que acessasse ilegalmente um computador unicamente com o objetivo de copiar programas sigilosos.

Em Portugal[46], o acesso ilegítimo foi tipificado pela Lei de Criminalidade Informática (lei nº 109) de 17 de agosto de 1991 que criminalizou a conduta de

---

[46] *"Art. 7º Acesso ilegítimo - 1. Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até um ano ou com pena de multa até 120 dias. 2. A pena será a de prisão até três anos ou multa se o acesso for conseguido através da violação de regras de segurança. 3. A pena será a de prisão de um a cinco anos quando: a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 4. A tentativa é punível. 5. Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa."* <http://www.terravista.pt/mussulo/1139/crimi.html>

quem, sem autorização, acede a um sistema ou redes informáticos com intenção de alcançar um benefício ilegítimo para si ou para outrem.

No Reino Unido[47], a conduta típica é dar causa a um computador executar função que atente contra o acesso protegido a programa ou dado armazenado em computador.

Na Suécia[48], a lei penal incrimina a conduta de quem ilegalmente obtém acesso a gravações de processamento automático de dados ou altera, apaga ou insere gravação semelhante em um registro. A pena prevista é de multa ou até 2 (dois) anos de prisão.

A lei penal sueca, ao tipificar o acesso não autorizado a computadores e a alteração de dados em um único dispositivo, reprovou com a mesma pena as condutas de quem acessa ilegalmente o sistema para simplesmente ler os dados e a de quem, não se contentando com a simples leitura, os modifica seja

---

[47] *"Unauthorised access to computer material. 1.—(1) A person is guilty of an offence if— (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case. (2) The intent a person has to have to commit an offence under this section need not be directed at— (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer. (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both."* <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm>

[48] *"Chapter 4 - On Crimes against Liberty and Peace - Section 9c - A person who, in cases other than those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years. A recording in this context includes even information that is being processed by electronic or similar means for use with automatic data processing. (Law 1998:206)"* <http://wings.buffalo.edu/law/bclc/sweden.pdf>

apagando, alterando ou inserindo novos dados.

Na Suiça[49], o acesso não autorizado a computadores é delito meramente subsidiário e só é aplicável quando o acesso se dá sem a intenção do agente de obter vantagem ilegal por meio dele. Nos casos em que se verifica o *animus lucrandi*, o agente será punido pelos dispositivos comuns do Código Penal aplicáveis à espécie.

Na Bélgica[50], aquele que, sem autorização, acessa ou se mantém em um sistema informático é punido com prisão de 3 (três) meses a 1 (um) ano e multa. Se a infração é cometida com intenção de fraude a pena é de 6 (seis) meses a 2 (dois) anos. Pune-se expressamente a tentativa.

Mas nem só nos Estados Unidos e na Europa há legislações tipificando o acesso não autorizado a sistemas computacionais.

---

[49] *"Art. 143 bis - Accès indu à un système informatique - Celui qui, sans dessein d'enrichissement, se sera introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part, sera, sur plainte, puni de l'emprisonnement ou de l'amende."* <http://www.admin.ch/ch/f/rs/3/311.0.fr.pdf>

[50] *"Titre IXbis. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes. Art. 550bis. §1 er . Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprison-nement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement. Si l'infraction visée à l'aline 'a 1 er , est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans. § 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement."*
<http://www.droit-technologie.org/fr/legislations/loi_criminalite_informatique_281100.pdf>.

No Canadá[51], quem, fraudulentamente e ilegalmente, obtém qualquer serviço computacional ou intercepta função de um sistema computacional está sujeito a prisão de até 10 (dez) anos.

A lei canadense procura definir exaustivamente os elementos normativos do tipo. Serviço computacional é entendido como o processamento, o armazenamento e a recuperação de dados. O conceito de interceptar inclui ouvir ou gravar uma função de sistema computacional, ou adquirir seu conteúdo, significado ou objetivo. E a definição legal de função inclui o controle lógico e aritmético, o apagamento, o armazenamento, a recuperação e a comunicação ou telecomunicação de um sistema computacional.

Na China[52], a lei penal protege contra o acesso não autorizado somente os computadores nos quais estão armazenadas informações concernentes a assuntos estatais, a arquitetura dos aparatos de defesa ou a ciência e tecnologia sofisticadas. A pena cominada é de até 3 (três) anos de prisão.

---

[51] *"342.1(1) Unauthorized use of computer - (1) Every one who, fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."* <ftp://insight.mcmaster.ca/pub/efc/cce.txt>.

[52] *"Article 285. Whoever violates state regulations and intrudes into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention."* <http://www.qis.net/chinalaw/prclaw60.htm>

No México[53], para que a conduta de acessar sem autorização um sistema computacional seja típica, é necessário que o sistema esteja protegido por algum mecanismo de segurança. Esta solução adotada pelo legislador mexicano transfere ao administrador do sistema o ônus pela sua guarda, presumindo que, se não há a devida proteção por parte dos técnicos responsáveis por salvaguardá-lo, não caberá também à norma penal proteger tais sistemas.

A solução mexicana é absurda, pois equipara a ausência de dispositivos de segurança no sistema à verdadeira publicidade dos dados lá armazenados. Seria como admitir-se que, para a ocorrência do crime de violação de domicílio, necessariamente as portas tenham que estar trancadas.

Na América Latina, o acesso não autorizado a sistemas computacionais só encontra-se tipificado no Chile[54] onde desde 1993 a conduta é típica.

Por fim, vale ressaltar que na Europa o acesso não autorizado a sistemas computacionais poderá ser, em breve, regulado por um tratado internacional. O

---

[53] *"Artículo 211 bis1 Al que sin autorizacion modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa."*

"Al que sin autorización conozca o copie información contenida em sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."
<http://www.cddhcu.gob.mx/leyinfo/pdf/11.pdf>

[54] *"Ley num. 19.223 - Ley relativa a delitos informaticos - Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio."* <http://chile.derecho.org/concepcion/~/legislacion/19223/>

Comitê Europeu para Problemas Delitivos (*European Committee on Crime Problems*) aprovou em junho de 2001 o *Draft Convention of Cybercrime*[55] que, se aprovado, tornar-se-á o primeiro tratado internacional sobre criminalidade informática do mundo. O texto é resultado de quatro anos de trabalho do Comitê e, para ser adotado, deverá antes ser aprovado pelo Comitê de Ministros do Conselho da Europa.

---

[55] *"Article 2 – Illegal access - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*
<http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>

5. DOS ELEMENTOS DA CONDUTA TÍPICA

Analisada a legislação estrangeira que disciplina o acesso não autorizado a sistemas computacionais, é fundamental que identifiquemos agora os elementos desta conduta típica.

Evidentemente que tais elementos irão variar de acordo com o ordenamento jurídico estudado. Não buscaremos aqui tratar destas especificidades, mas sim estabelecer os elementos comuns das condutas típicas de acesso não autorizado a sistemas computacionais.

Uma vez que, até a presente data, o acesso não autorizado a computadores ainda não foi tipificado no ordenamento jurídico brasileiro, basearemos nossa análise em um tipo hipotético que, no nosso entender, melhor disciplinaria a matéria em nosso sistema penal. Eis sua redação:

> ***Acessar sem autorização dados ou programas em sistema computacional.***

Os conceitos de dados e programas já foram analisados neste trabalho e está claro que constituirão o objeto material do delito ora em estudo.

Resta-nos, então definir o que se deve entender pelo núcleo da conduta típica – verbo acessar – e pelos elementos normativos *sem autorização* e *sistema computacional*.

FRAGOSO ensina que:

> *"São elementos descritivos aqueles cujo conhecimento se*

> *opera através de simples verificação sensorial, o que ocorre quando a lei se refere a membro, explosivo, parto, homem, mulher, etc. A identificação de tais elementos dispensa qualquer valoração."*
>
> *"Ao lado de tais elementos encontramos os chamados normativos, que só podem ser determinados mediante especial valoração jurídica ou cultural."* (FRAGOSO, 1985. p. 163)

É fácil perceber que os elementos *sem autorização* e *sistema computacional* necessitam de uma valoração alheia ao Direito Penal para sua perfeita compreensão. Não são conceitos ônticos, pois o primeiro está diretamente relacionado à idéia jurídica de posse característica do Direito Privado e o segundo baseia-se em um conceito técnico próprio da Ciência da Computação.

A redação de tipos penais, em princípio, deveria ser primordialmente realizada com elementos descritivos, pois como bem lembram ZAFFARONI e PIERANGELI:

> *"O tipo é predominantemente descritivo, porque os elementos descritivos são os mais importantes para individualizar uma conduta e, dentre eles, o verbo tem especial significação, pois é precisamente a palavra que gramaticalmente serve para conotar uma ação."* (ZAFFARONI et PIERANGELI, 1997. p. 444)

Um tipo penal com muitos elementos normativos poderia significar uma séria ameaça de lesão à segurança jurídica, uma vez que estes dependem de valoração dos aplicadores da norma.

Nos delitos informáticos, contudo, o uso de elementos normativos no tipo parece ser inevitável, por sua própria natureza tecnológica que vincula a

interpretação da norma às modernas criações da Ciência da Computação.

Caberá ao aplicador da norma interpretar tais elementos normativos de forma restritiva, pois como bem lembra MAXIMILIANO:

> *"Estritamente se interpretam as disposições que restringem a liberdade humana, ou afetam a propriedade; conseqüentemente, com igual reserva se aplicam os preceitos tendentes a agravar qualquer penalidade. O contrário se observa relativamente às normas escritas concernentes às causas que justificam os fatos delituosos e dirimem ou atenuam a criminalidade: devem ter aplicação extensiva desde que os motivos da lei vão além dos termos da mesma; em tais circunstâncias, até a analogia é invocável."* (MAXIMILIANO, 1997. p. 322)

Procuraremos, a seguir, definir cada um destes conceitos normativos, bem como o significado do próprio núcleo da conduta típica – acessar – buscando na Ciência da Computação os subsídios necessários para tanto.

5.1. Sistemas computacionais

Sistema computacional[56] [57] é um conjunto de dispositivos interconectados

---

[56] O *Draft Convention On Cyber-Crime* define em seu art. 1º: *"'computer system' means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data."*
<http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>.

[57] *"No século XVII os franceses criaram o verbo computer (com acento tônico no e), com o sentido de calcular, mas foram os ingleses que transformaram o verbo no substantivo computer (com acento tônico no u), para designar as primitivas máquinas que hoje chamamos calculadoras. A aplicação do termo ao moderno computador só aconteceria a partir de 1944, quando o jornal inglês London Times publicou uma então delirantíssima matéria sobre alguns equipamentos inteligentes que no futuro poderiam a vir a substituir o esforço humano. O Times*

capaz de processar dados automaticamente.

O termo automaticamente significa que o processamento se dá sem a intervenção direta de seres humanos. É como se alguém, para fazer um bolo, entregasse uma receita a um robô e o mandasse seguir aquelas instruções.

A intervenção humana limitou-se à criação das ordens a serem seguidas e ao comando para que as executassem. Após o comando, isto é, durante a execução, não há mais qualquer necessidade de intervenção humana, daí por que chamaremos este sistema de automático.

Está claro também que o sistema é formado por dois elementos bem distintos: o robô e a receita. O primeiro, um sistema eletrônico apto a receber instruções, o qual chamaremos de *hardware*. O segundo as próprias instruções, ou seja, os programas, que chamaremos de *software*.

Assim, é fácil perceber que tanto um simples computador doméstico como um sofisticado computador de grande porte são sistemas computacionais formados por uma série de dispositivos físicos interconectados (processador, memória, disco rígido, etc.) comandados por uma série de dispositivos lógicos (BIOS[58], sistema operacional, programas utilitários).

---

chamou uma hipotética máquina pensante de computer." (GEHRINGER et LONDON, 2001, p. 14).

[58] *"BIOS (Basic Input/Output System – Sistema Básico de Entrada/Saída): "Ensina" o processador a trabalhar com os periféricos mais básicos do sistema, tais como os circuitos de apoio, a unidade de disquete e o vídeo em modo texto."* (TORRES, 1999. p. 11)

Na atualidade, estamos cercados por sistemas computacionais: telefone celular, forno de microondas, televisão, videocassete, calculadora, agendas eletrônicas, caixas bancários automáticos e, evidentemente, os computadores pessoais.

As estações de trabalho, servidores e computadores de grande porte, em sua essência, em nada diferem dos sistemas computacionais citados acima, tendo como diferencial apenas o nível de complexidade de seus mecanismos físicos (*hardware*) e lógicos (*software*).

Interessante é notar que, se interconectarmos dois ou mais sistemas computacionais teremos como resultado um novo e único sistema computacional como resultado da fusão dos anteriores.

Isto se dá porque, como já mencionado, sistemas computacionais são conjuntos de dispositivos interconectados capazes de processar dados automaticamente. Ora, a interconexão de dois ou mais conjuntos destes dispositivos os fundirá num único conjunto de dispositivos um tanto quanto mais complexo, mas em essência suas características não se terão alterado.

Voltando à analogia dos robôs cozinheiros, se alguém confia a tarefa de se fazer um bolo a dois robôs, poderia dividir as funções entre eles. Um ficaria encarregado de fazer a massa e o outro a cobertura. Para cada um deles seria também entregue uma receita com as instruções específicas da sua função.

Os dois robôs trabalhando com base nas duas receitas poderiam ser considerados um sistema computacional, mas também cada um deles com sua

receita específica também seria um sistema computacional.

Paradoxalmente, no entanto, os sistemas computacionais originais continuam existindo autonomamente dentro do sistema computacional maior originado de suas fusões.

Conclui-se que um sistema computacional é um conjunto de dispositivos físicos e lógicos interconectados que tem como objetivo principal armazenar e processar dados automaticamente.

5.2. Redes

Redes[59] são sistemas computacionais formados pela interconexão de dois ou mais sistemas computacionais menores. Esta interconexão pode se dar por fios, cabos, por ondas de rádio, infravermelho ou via satélite.

As redes serão classificadas, de acordo com área de sua abrangência, em redes locais (LAN - *local area network*), usadas em residências e escritórios, e redes de área ampliada (WAN - *wide area network*), usadas para interconectar redes locais.

---

[59] *"A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols."* <http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm>.

A Internet é uma rede global que consiste na interconexão de inúmeras redes que usam todas o mesmo protocolo[60].

Cada um dos computadores desta rede recebe um endereço consistente de 32 bits divididos em quatro campos de um byte (oito bits) cada, variando, pois, de 0 a 255. Por exemplo:

32.104.87.2

150.164.76.80

198.186.203.18

Este endereço, denominado IP, é único na rede e identifica cada um dos computadores interconectados.

A manipulação de tais endereços numéricos é, no entanto, muito pouco prática, razão pela qual existe o Sistema de Nomes de Domínio (DNS – *Domain Name System*) que relaciona cada um dos endereços IPs a nomes específicos, denominados domínios.

É possível fazer-se uma analogia com o sistema de nomes usado pelo Direito Comercial, no qual a empresa cuja razão social é "Silva e Santos Ltda." pode adotar um nome fantasia para se apresentar ao consumidor como "Sorveteria Gelada". De forma semelhante, o endereço 200.100.50.1 é associado ao

---

[60] Um protocolo é um conjunto de regras que regula a transmissão de dados entre computadores.

dominio www.dominio.com.br , para facilitar sua memorização pelo grande público. Eis alguns exemplos:

32.104.87.2 = www.stf.gov.br

150.164.76.80 = www.ufmg.br

198.186.203.18 = www.gnu.org

Em tese, uma única lista contendo a relação de todos os domínios da Internet, relacionados a seus respectivos IPs, poderia ser armazenada em um servidor central que ficaria responsável pela "tradução" dos domínios. Na prática, porém, esta se revelaria uma solução desastrosa, pois a rede ficaria completamente vulnerável a um ataque a este servidor responsável pelo rol de domínios.

A solução encontrada foi a criação de um sistema descentralizado e hierarquizado para gerir a relação entre domínios e endereços IPs. Assim, o nome de domínio, que em princípio poderia ser formado de uma única palavra, passou a obedecer a um formato hierarquizado, no qual a maior hierarquia encontra-se à direita e diminui progressivamente até a menor hierarquia, encontrada à extrema esquerda.

Retornando ao exemplo, www.dominio.com.br tem como maior hierarquia o domínio *br*, como segunda hierarquia o domínio *com*, como terceira, *domínio* e como quarta e menor hierarquia, *www*.

Assim, quando o usuário digita o endereço www.dominio.com.br em seu

programa navegador, este procura na rede o servidor de nomes responsável por gerenciar os domínios *.br*, que o remeterá ao servidor de nomes que gerencia os domínios *.com.br* que por sua vez enviará a requisição a um outro servidor que gerencie o *.dominio.com.br* que finalmente irá indicar o endereço IP do computador *www.* [61]

Os domínios de mais alta hierarquia na Internet são denominados TLDs (*Top-Level Domain Names*) e representam o código do país de origem da página, identificado por 2 letras (padrão ISO), *v.g.* br, fr, us, uk, jp, e outros[62].

O domínio brasileiro é o .br que, por sua vez, encontra-se dividido em inúmeros domínios de 2º nível, dentre os quais destacam-se: com.br (comerciais), org.br (entidades não governamentais sem fins lucrativos), nom.br (pessoas físicas), ind.br (indústrias), adv.br (advogados), med.br (médicos), entre outros[63].

---

[61] Nada impede, no entanto, que em qualquer dos servidores de hierarquia superior haja a lista com a relação do nome de domínio completo e seu endereço IP.

[62] Na prática, a maioria das páginas originárias dos EUA não adota o *.us*, simplesmente terminando em .com (organizações comerciais), .edu (instituições educacionais), .gov (instituições governamentais), .mil (agências militares), .net (serviços da rede) e .org (organizações não comerciais), gerando a falsa impressão de que estes domínios de segundo nível são TLDs.

[63] A lista completa dos domínios brasileiros pode ser encontrada em www.registro.br

5.3. Acessos

Acesso é a ação humana de ler, escrever[64] ou processar dados armazenados em sistemas computacionais.

Ler dados armazenados em um sistema computacional consiste em reinterpretá-los como informações humanamente inteligíveis. A leitura de um texto, a visualização de fotos e a audição de músicas armazenadas em computador são exemplos de leitura de dados.

A escrita, em sentido amplo, consiste na inserção, remoção ou alteração de dados no sistema.

Pode se dar tanto em memórias voláteis[65] – aquelas nas quais os dados são apagados quando o sistema é desligado – quanto em memórias graváveis.

Praticamente qualquer contato de um ser humano com um computador é um acesso. Se se lê uma informação exibida em um monitor recuperam-se dados; se se clica com o *mouse* em algum ponto da tela ou pressiona-se a barra de espaço do teclado, inserem-se dados; se se altera o nome de um arquivo, modificam-se dados; se se desliga o computador, apagam-se dados da

---

[64] Escrever – *"Inform. Comunicar ou introduzir (informações) em alguma parte da memória, seja em fitas magnéticas, seja em discos magnéticos."* (FERREIRA, 1999)

[65] Volátil - Inform. *"Diz-se de dispositivo de memória cujo conteúdo se perde na ausência de tensão elétrica de alimentação, como, p. ex., a RAM."* (FERREIRA, 1999)

memória RAM[66].

O acesso pode ser local ou remoto. O acesso é local quando a conduta humana se dá no mesmo sistema computacional no qual estão armazenados os dados. O acesso é remoto quando os dados encontram-se num sistema computacional diverso daquele em que a ação humana é realizada, estando os dois sistemas interconectados em rede.

Exemplos de acessos remotos são a visita a uma página da Internet ou o envio de um email. No primeiro caso há um acesso de leitura dos dados (a página que se visualiza) no computador remoto e no segundo caso há um acesso de escrita de dados (o texto do email) no servidor remoto.

5.4. Permissões de acesso

Permissões são atributos[67] que controlam o acesso a arquivos e diretórios de um sistema computacional.

---

[66] RAM (Random-Access Memory) – Memória de acesso randômico, permite que o usuário leia e também armazene informações (leitura e escrita). Em compensação seu conteúdo é perdido sempre que são desligadas (são voláteis). O nome randômico é uma alusão a sua capacidade de interação com o usuário: *"A palavra random tem origem francesa –randir – e antigamente significava galopar sem destino. Depois, foi adotada pela Estatística para definir qualquer fato que acontece ao sabor do acaso, sem método, como os números da Mega Sena, por exemplo. Daí, entrou para o ramo da computação, com o sentido de você decide."* (GEHRINGER et LONDON, 2001, p. 37)

[67] Aqui o vocábulo atributo é usado com o significado próprio de: *"Inform. Item de informação indivisível, em arquivo, banco de dados, ou na modelagem conceitual."* (FERREIRA, 1999)

As permissões podem ser de leitura, escrita e execução[68] e cada usuário terá diferentes níveis de acesso em relação aos vários arquivos e diretórios do sistema.

Diferentes usuários de um sistema terão níveis de permissão diversos para cada arquivo. Suponhamos um arquivo texto qualquer armazenado em um sistema computacional. Alguns usuários terão permissão para lê-lo, porém sem a possibilidade de alterá-lo. Outros terão permissão de leitura e escrita, podendo lê-lo e modificá-lo (acrescentar, modificar, ou mesmo apagar conteúdo). Haverá ainda aqueles sem qualquer permissão de acesso e estes não poderão nem lê-lo nem alterá-lo.

O usuário que criou o arquivo no sistema computacional, em princípio, terá plenos poderes em relação ao arquivo criado, podendo lê-lo, alterá-lo e, caso seja um programa ou um script, executá-lo. Aos demais, na maioria das vezes, é permitida somente a leitura do arquivo, quando muito.

Assim, quando acessamos uma página na Internet, esse acesso se dá com permissão somente para leitura, não havendo, pois, permissão para que efetuemos qualquer modificação em seu conteúdo.

---

[68] Somente programas ou scripts podem ter permissão para serem executados.

5.5. Autorização de acesso

Autorização é a legitimidade jurídica que alguém possui para acessar determinados dados em um sistema computacional.

Sua validade decorre da propriedade dos dados e o proprietário dos dados, evidentemente, terá sempre plenos poderes para acessá-los. Poderá ele também permitir que outras pessoas tenham acesso a esses dados, autorizando-as, geralmente através da concessão de uma senha.

Presume-se que aquele que tenha a permissão para acessar um arquivo também tenha autorização do proprietário para fazê-lo.

Ocorre, no entanto, que, em determinados casos, a pessoa tem o poder de fato de acessar os dados – permissão de acesso – porém não tem a autorização juridica do proprietário para fazê-lo.

É o que ocorre nos casos de excesso no acesso autorizado a computadores.

5.6. Excesso no acesso autorizado

Em todo sistema computacional há a figura do superusuário (*root*) que é plenipotenciário em relação a todos os arquivos armazenados no sistema e também em relação a todos os seus recursos. O superusuário é o administrador do sistema operacional e, como tal, controla o sistema computacional, podendo ler, escrever (acrescentar, modificar, apagar) ou

executar qualquer arquivo nele contido.

A autorização de acesso que o superusuário tem em relação a todos os arquivos do sistema não implica em um reconhecimento jurídico de poderes arbitrários a ele. Sua autorização de acesso pleno é meramente operacional e se limita às necessidades próprias de administração do sistema.

Seus atos no uso desta autorização plena só serão legítimos quando necessários para a correta operação do sistema. Ainda que tecnicamente ele tenha permissão para acessar qualquer dos dados armazenados no sistema, juridicamente sua autorização está limitada à necessidade e aos fins deste acesso.

Se é certo que o superusuário tem permissão para ler qualquer email armazenado no sistema, certo é também que não pode estar ele juridicamente autorizado a fazê-lo tão-somente para satisfazer sua curiosidade, pois haveria, no caso, uma clara ofensa ao bem jurídico inviolabilidade dos dados.

Todo e qualquer acesso do superusuário a arquivos a ele não pertencentes que não vise à operação do sistema deve ser considerado um excesso do acesso autorizado ao sistema computacional. O administrador do sistema deverá responder, pois, pelo excesso no uso de sua permissão de acesso pleno ao sistema.

5.7. Insignificância penal do acesso não autorizado

O envio de um email é um acesso remoto de escrita no qual o remetente grava o conteúdo do email no computador do destinatário. A permissão e autorização do destinatário é somente de escrita e é presumida no momento em que alguém de qualquer forma disponibiliza seu endereço eletrônico.

Ocorre, no entanto, que é prática bastante comum na Internet o envio de emails publicitários[69] para pessoas que nunca ofereceram seus endereços eletrônicos para este fim.

Os remetentes destes emails indesejados têm permissão de escrita no computador da vítima, ainda que esta não tenha autorizado o envio de tais mensagens.

Os endereços eletrônicos são adquiridos pelas mais diversas formas e não é difícil encontrar quem venda em CDs-ROMs verdadeiros catálogos de emails.

Evidentemente que, se os destinatários destes emails não cederam seus endereços para quem enviou tais mensagens publicitárias, não há sequer uma autorização tácita que justifique a escrita destes dados em seu computador, o que, em tese, tipificaria o acesso não autorizado a sistemas computacionais.

Tal prática, ainda que profundamente condenável, não parece ofender com o

---

[69] Esta prática é conhecida como *"spam"*.

grau de gravidade necessária o bem jurídico inviolabilidade dos dados, razão pela qual a conduta será considerada atípica pela aplicação do princípio da insignificância.

Na interpretação das normas penais não se pode olvidar que os tipo penais, para serem materialmente válidos, devem fundamentar-se na proteção de um bem jurídico socialmente relevante.

O Direito Penal é remédio extremo que a sociedade reconhece ter conseqüências colaterais extremamente gravosas não só para o condenado, mas também para ela própria.

O reconhecimento desta subsidiaridade do Direito Penal remonta ao Direito Romano no qual já se afirmava que *minima non cura praeter.*

A necessidade de haver uma proporção entre o delito praticado e a pena aplicada foi ressaltada por BECCARIA no século XVIII:

> *"Não somente é interesse de todos que não se cometam delitos, como também que estes sejam mais raros proporcionalmente ao mal que causam à sociedade. Portanto, mais fortes devem ser os obstáculos que afastam os homens dos crimes, quando são contrários ao bem público e na medida dos impulsos que os levam a delinqüir. Deve haver, pois, proporção entre os delitos e as penas."* (BECCARIA, 1999. p. 37)

A insignificância da afetação do bem jurídico foi retomada, modernamente, por vários autores, destacando-se dentre eles Claus Roxin que em sua célebre obra Política Criminal e Sistema Jurídico Penal, publicada na Alemanha em 1970, tomou-o como "*auxílio de interpretação para restringir formulações*

literais que também abranjam comportamentos suportáveis." (ROXIN, 2000. p.47)

A palavra-chave para a correta compreensão do princípio da insignificância é **suportável**. Não se trata de uma conduta elogiável, nem mesmo neutra, mas que o Estado se vê obrigado a suportar em razão da evidente desproporção entre a conseqüência legal prevista (pena) e o comportamento indesejado.

Assim, por mais que a prática do *"spam"* seja condenável, não poderá ela gerar conseqüências penais, uma vez que a ofensa ao bem jurídico não é suficientemente relevante para justificar a aplicação de uma sanção penal. Suas conseqüências deverão restringir-se, pois, ao âmbito privado.

Também deverá ser considerado um acesso não autorizado insignificante para efeitos penais o uso de *cookies*[70] em páginas da Internet. Tal prática, freqüente em grande números de sites, consiste na gravação de um pequeno arquivo contendo informações a respeito deste usuário que acessa determinada página da Internet.

O uso deste dispositivo é freqüente em páginas de comércio eletrônico. Ao efetuar a compra de um livro jurídico, por exemplo, o *site* grava o nome do livro comprado no computador do comprador para que, ao visitá-lo novamente, este possa ser assediado com anúncios publicitários direcionados, oferecendo-lhe

---

[70] Do inglês – biscoitos. São pequenos arquivos-textos gravados no computador da vítima, contendo suas informações pessoais e, em geral, seus hábitos de consumo.

novos livros jurídicos.

É bem verdade que os programas navegadores permitem a desabilitação desta função que autoriza a gravação dos *cookies* no sistema, mas a maioria dos usuários sequer conhece esta possibilidade e acaba sendo induzida a aceitar – não permitir – o acesso pelo completo desconhecimento técnico do sistema.

A discussão da propriedade do uso de tais dispositivos, deve, no entanto, também limitar-se à esfera cível, pois sua utilização não afeta o bem jurídico inviolabilidade dos dados informáticos com a gravidade necessária para a justificação de uma sanção penal.

6. DO TEMPO E DO LOCAL DO DELITO

Vistos os elementos fundamentais da conduta típica, procuraremos determinar, neste capítulo, o momento e o local da consumação do delito, bem como suas conseqüências no Direito Penal e no Direito Processual Penal.

Para tanto, buscaremos definir, *ab initio,* qual o resultado fenomênico produzido pela conduta de acesso não autorizado a sistemas computacionais.

6.1. Crimes materiais, formais e de mera conduta

Todo crime, por sua própria definição, tem como resultado jurídico uma ofensa a um bem penalmente tutelado. No acesso não autorizado a computadores este bem é a inviolabilidade dos dados.

Além do resultado jurídico, os crimes também geram resultados materiais, isto é, alterações no mundo fenomênico.

Muitos doutrinadores classificam os crimes quanto ao resultado material que produzem em delitos materiais, formais e de mera conduta.

Segundo tais autores, delitos materiais são aqueles em que ocorre um resultado no mundo fenomênico penalmente relevante; delitos formais são aqueles em que ocorre um resultado no mundo fenomênico penalmente irrelevante e delitos de mera conduta são aqueles em que não ocorre resultado

no mundo fenomênico.

Acreditamos que tal classificação é muito mais uma sistematização das diversas técnicas legislativas usadas para descrever uma conduta que uma diferenciação ontológica dos crimes.

ZAFFARONI e PIERANGELI afirmam que:

> *"O que ocorre é que todos os tipos requerem um resultado, só que os individualizam de maneiras distintas: alguns os mencionam expressamente, outros vinculam-nos inseparavelmente à conduta, outros preferem limitar-se ao puro resultado da conduta, desinteressando-se de qualquer outro que possa causar."* (ZAFFARONI e PIERANGELI, p. 471).

Assim, o delito de mera conduta "atravessar uma ponte" poderia ser redigido como delito material nos seguintes termos: "dirigir passos para o lado oposto da ponte até atingir o seu final". Trata-se, pois, de mera opção de redação adotada pelo legislador a distinção entre delitos materiais e de mera conduta.

Nos delitos formais, por outro lado, ocorre efetivamente um resultado no mundo fenomênico, porém este resultado é irrelevante para a tipificação do delito. No delito de injúria, *verbi gratia*, é irrelevante que o agente consiga alcançar o resultado pretendido – a vítima se sentir ofendida – pois a norma não toma este resultado como essencial para a tipicidade da conduta. O resultado fático, porém, existe e se resume a duas hipóteses antagônicas: a vítima sentir-se ofendida (resultado fático pretendido pelo agente) ou a vítima tomar conhecimento da ofensa, porém não se deixar ofender (resultado fático diverso daquele pretendido pelo agente).

Se em todo crime há um resultado fático, resta-nos saber qual é o resultado material produzido pelo acesso não autorizado a sistemas computacionais e se ele é relevante ou não para a caracterização da tipicidade da conduta.

Vimos que o acesso é a conduta de ler, escrever ou processar dados em sistemas computacionais. Há, pois, três modalidades distintas do delito de acesso não autorizado a sistemas computacionais, sendo que em cada uma delas encontraremos um par ordenado de ação e resultado.

Nas três modalidades a ação será sempre um comando emitido pelo agente, geralmente digitado em um teclado, podendo ser emitido também através de um *mouse*, um microfone ou qualquer dispositivo de entrada de dados. Este comando processará uma série de instruções que gerará um dos três resultados que caracterizam a modalidade do acesso.

Quando alguém emite um comando para que um editor de textos abra um arquivo, o sistema processará uma série de instruções que irá acarretar como resultado a exibição do texto no monitor. Do mesmo modo, a impressão de uma foto ou a audição de um arquivo de som. Esta é a modalidade de leitura de dados.

Quando alguém emite um comando para que o sistema apague um arquivo ou salve as alterações nele efetuadas também ocorrerá uma seqüência ordenada de instruções que gerarão uma modificação dos dados originariamente armazenados no sistema. Esta é a modalidade de escrita de dados.

Quando alguém emite um comando para que o computador inicialize o editor

de textos ou abra um jogo de computador, desencadeia um processo que culminará com a execução do programa. Esta é a modalidade de processamento de dados.

Constata-se claramente que a proteção penal deverá incidir sobre a leitura, a escrita ou o processamento dos dados e não sob a simples emissão do comando sem a ocorrência do resultado.

Em uma analogia com o crime de homicídio, poderíamos afirmar que a digitação do comando ou o clicar do *mouse* equivalem ao disparo de uma arma e a leitura, escrita ou processamento dos dados equivalem à morte da vítima.

Assim como matar equivale semanticamente a produzir lesões corporais em outrem, causando-lhe o resultado morte, acessar significa emitir comandos a um sistema computacional, causando a leitura, a escrita ou o processamento de dados.

O delito de acesso não autorizado a sistemas computacionais é, portanto, crime material, já que o resultado fático da conduta é penalmente relevante.

Esta conclusão é fundamental no estudo da tentativa, do tempo e local do delito e da co-autoria e participação.

6.2. Tempo do crime

A determinação do exato momento da ocorrência do crime é importante na

aplicação da norma penal para a solução de conflito temporal de normas, aferição da imputabilidade do agente, aplicação da anistia e da prescrição e análise das circunstâncias do crime.

Destacam-se três teorias doutrinárias a este respeito: a teoria da atividade ou da ação, segundo a qual o crime é praticado no momento da execução da conduta; a teoria do resultado ou do evento, pela qual o crime considerar-se-á realizado no momento de seu resultado; a teoria mista ou unitária, em que o crime é considerado cometido tanto no momento da conduta quanto no de seu resultado.

O art. 4º do CP adotou a teoria da ação ou da atividade e estabeleceu que:

> *"considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado."*

Antônio José Fabrício LEIRIA acentua que:

> *"É exatamente no instante da ação que a inteligência que pensa e a vontade que quer se manifestam no mundo exterior, tornando-se relevantes ao direito. É neste momento da ação ou omissão que se objetiva o querer do agente e, portanto, revela-se a sua rebeldia ao comando da lei. Logo, aqui é que se deve situar o tempus delicti."* (LEIRIA, Antônio José Fabrício. *Teoria e prática da lei penal*, 1981. p.93-94 *apud* FRANCO et al., 1987. p. 13)

Há que se observar aqui que, nos delitos informáticos em geral, muita vez, o período de tempo entre a ação e o resultado é relativamente grande. Isto porque, ao digitarmos determinado comando em um computador ligado em rede, para que ele execute uma operação em outra máquina, provavelmente tal instrução viajará por muitos cabos até chegar a seu destino.

Nos casos em que o agente opta por transferir o arquivo inteiro do computador da vítima para o seu (*download*[71]), esta operação poderá levar horas, mas o delito será considerado praticado no momento em que foi dado o comando para a transferência.

É perfeitamente possível ainda que o acesso não autorizado a sistemas computacionais seja praticado como delito permanente. Basta que o agente, ao obter o acesso, troque a senha do sistema, impedindo os acessos do(s) usuário(s) autorizado(s) e garantindo novos acessos futuros até que providências sejam tomadas. A ação e o resultado, neste caso, prolongar-se-ão até que o legítimo proprietário consiga reaver o controle do sistema.

6.3. Local do crime

Diversos são os posicionamentos doutrinários acerca da fixação do *locus commissi delicti*. PRADO enumera as seguintes teorias:

> *"a)teoria da ação ou da atividade: lugar do delito é aquele em que se realizou a ação ou a omissão típica; b) teoria do resultado ou do efeito: lugar do delito é aquele em que ocorreu o evento ou o resultado; c) teoria da intenção: lugar do delito é aquele em que devia ocorrer o resultado, segundo a intenção do autor; d) teoria do efeito intermédio ou do efeito mais próximo: lugar do delito é aquele em que a energia movimentada pela atuação do agente*

---

[71] *"[Ingl., de down(line), 'linha abaixo (i. e., seguindo o fluxo de informações)', + load, 'carga', 'ato de carregar'.] Numa rede de computadores, obtenção de cópia, em máquina local, de um arquivo originado em máquina remota."* (FERREIRA, 1999)

> *alcança a vítima ou o bem jurídico; e) teoria da ação a distância ou da longa mão: lugar do delito é aquele em que se verificou o ato executivo; f) teoria limitada da ubiqüidade: lugar do delito tanto pode ser o da ação como o do resultado; e g) teoria pura da ubiqüidade, mista ou unitária: lugar do delito tanto pode ser o da conduta como o do resultado ou o lugar do bem jurídico atingido."* (PRADO, 2000. p. 111)

O Código Penal Brasileiro consagrou a teoria pura da ubiqüidade ao dispor em seu art. 6º que:

> *"considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado."*

A aplicação desta norma aos casos de acessos não autorizados a computadores cometidos através da Internet em que o computador do agente encontra-se em país diferente do da vítima é demasiadamente simples quando em ambos os países o acesso não autorizado a sistemas computacionais é fato típico.

Nestes casos, supondo que o acesso não autorizado a computadores já fosse típico em nossa legislação, poder-se-ia punir o agente tanto quando acessasse a partir de um computador localizado no Brasil um sistema localizado no estrangeiro quanto, ao contrário, uma vítima no Brasil sofresse um ataque proveniente de um computador localizado em outro país.

Bem mais complexas, no entanto, serão as soluções a serem dadas quando a conduta é típica em apenas um dos países.

Assim, pode ocorrer que a conduta seja típica no país em que o comando é

dado, porém atípica no Estado onde se dá o resultado fático. Ou, ao contrário, ser atípica no país da ação e típica no do resultado fenomênico.

Para encontrarmos a solução para estas duas situações devemos partir do pressuposto de que as normas de caráter penal são interpretadas restritivamente. Assim, havendo duas interpretações possíveis e perfeitamente lógicas para uma mesma situação jurídica, deverá o intérprete optar por aquela que menos restringir a liberdade do cidadão.

Ora, o art. 6º do CP, traz em sua redação a palavra "crime" e não "ação" ou "conduta". Se o crime será considerado praticado tanto no local da conduta quanto no lugar do resultado, necessário se faz que, para ser considerado crime, seja crime tanto no local da conduta quanto no do resultado.

Fundamental, pois, que esteja tipificado em ambas as legislações, sob pena de ofensa direta ao princípio constitucional do *nullum crimen sine lege*.

Se é a própria norma que estabelece a ubiqüidade como característica do crime (será crime no lugar da conduta e no local do resultado), por um raciocínio reverso podemos entender que só será crime se for crime no lugar da conduta e no local do resultado.

Raciocinar de forma contrária é admitir a paradoxal hipótese de um crime que não obedece a norma estabelecida no art. 6º do CP, pois só seria crime no local da conduta ou no do resultado, sendo no outro conduta lícita.

Nos casos específicos das condutas realizadas no Brasil, que são típicas em nossa legislação, mas que produzem resultados em países onde são atípicas,

aplica-se também o princípio da exclusiva proteção a bens jurídicos.

Se um Estado soberano entende ser desnecessária a proteção de determinado bem jurídico, não pode o Brasil querer protegê-lo, quando o resultado típico se dá nas fronteiras deste país, sob pena de autêntica violação ao art. 4º, III da Constituição Federal[72].

6.4. Jurisdição e competência

A palavra jurisdição deriva-se da união de duas palavras latinas: *ius, iuris* (direito) e *dictio,dictionis* (ação de dizer), podendo ser traduzida literalmente como a arte de dizer o direito. Segundo MANZINI:

> *"Jurisdição é a função soberana, que tem por escopo estabelecer, por provocação de quem tem o dever ou o interesse respectivo, se, no caso concreto, é aplicável uma determinada norma jurídica; função garantida, mediante a reserva do seu exercício, exclusivamente aos órgãos do Estado, instituídos com as garantias da independência e da imparcialidade (juízes e da observância de determinadas formas (processo, coação indireta)."* (MANZINI, *Trattato di diritto processuale penale italiano secondo il nuovo Codice*, 1931.v. 2, p. 19 *apud* CAPEZ, 2000. p. 177)

A jurisdição é, pois, junto com o poder de legislar e de governar, a expressão da soberania de um Estado. Este poder é uno, mas a sua aplicação, por uma

---

[72] *"Art. 4º - A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: (...) III – autoderterminação dos povos."*

questão de ordem prática, é repartida entre vários órgãos do corpo estatal.

MIRABETE ensina que:

> *"Como poder soberano do Estado, a juridição é una e, investido do poder de julgar, o juiz exerce a atividade jurisdicional. Sendo evidente, porém, que um juiz não pode julgar todas as causas e que a jurisdição não pode ser exercida ilimitadamente por qualquer juiz, o poder de julgar é distribuído por lei entre os vários órgãos do Poder Judiciário, através da competência. A competência, é assim, a medida e o limite da jurisdição."* (MIRABETE, 1999. p. 136)

A competência é pois o limite do poder de cada órgão jurisdicional. A distribuição dos poderes jurisdicionais do estado se dá de acordo com a natureza do crime praticado (*ratione materiae*), com a qualidade das pessoas incriminadas (*ratione personae*) e com o local em que o delito foi praticado ou consumou-se, ou ainda, com o local da residência de seu autor (*ratione loci*). Interessa-nos aqui a fixação da competência em razão da matéria e em razão do local do delito.

A Constituição Federal Brasileira, em seu art. 109, IV, fixa a competência dos juízes federais em razão da matéria, isto é, da natureza dos delitos praticados:

> *"os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral."*

A Internet é um serviço público de telecomunicação e como tal, sujeita-se à regulamentação da ANATEL (Agência Nacional de Telecomunicações), sendo o interesse da União em sua proteção jurídica incontestável. A Carta Magna

determina em seu art. 21, XI, que:

> *"Compete à União explorar, diretamente ou mediante autorização, concessão ou permissão, o serviços de telecomunicações, nos termos da lei, que disporá sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais."*

Assim, os processos relativos a acessos não autorizados a sistemas computacionais, quando praticados na Internet, deverão ser conhecidos e julgados pela Justiça Federal, uma vez que a Internet é um serviço da União.

Por outro lado, a competência será da Justiça Comum, quando o agente não se utilizar da Internet para obter o acesso não autorizado ao sistema computacional.

Quanto à competência em razão do local da infração, o art. 70 do Digesto Processual Penal brasileiro, ao contrário do Código Penal, não adotou a teoria da ubiquidade, mas sim a teoria do resultado.

Assim, a competência *ratione loci* para se julgar o delito de acesso não autorizado a computadores será fixada não pelo local onde foi dado o comando, mas sim, pelo local onde se encontre o sistema computacional indevidamente acessado.

Nos casos em que o sistema computacional estiver localizado no Brasil, a competência será do juízo deste local. Se, porém, o comando foi dado a partir de um sistema computacional localizado no Brasil e resultou em um acesso não autorizado em computadores de outro país, a competência será do juízo do local onde foi dado este comando, aplicando-se aqui o disposto no art. 70, §

1º do Código de Processo Penal Brasileiro que dispõe:

> *"Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução."*

Da mesma forma será fixada a competência nos casos de tentativa, quando, tendo sido dado o comando no Brasil, não tenha se consumado no estrangeiro por motivos alheios à vontade do agente. A competência será do juízo do local em que foi praticado o último ato de execução (art. 70, *caput*, do CPP).

Se, no entanto, o delito foi tentado no estrangeiro e seus resultados seriam produzidos no Brasil, aplica-se o disposto no § 2º do art. 70 do CPP:

> *"Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir o resultado."*

Assim, nestes casos a competência será do juízo onde estiver localizado o sistema computacional que foi ameaçado pela tentativa proveniente de país estrangeiro.

7. Do *iter criminis*

A teoria da tentativa remonta aos praxistas que conceberam a conduta criminosa como um caminho percorrido pelo agente (*iter criminis*). Assim, em toda conduta criminosa é possível vislumbrar as seguintes fases: cogitação (*cogitatio*), preparação (*conatus remotus*), execução (*conatus proximus*) e consumação (*meta optata*).

7.1. Da cogitação e da preparação

Evidentemente, a fase da cogitação não pode ser punida (*cogitationis poenam nemo patitur*), pois, caso contrário, estar-se-ia admitindo a punição pelos pensamentos do autor.

Assim, jamais um acesso não autorizado a computadores poderá ser considerado tentado pela simples declaração de alguém de que pretende invadir um determinado sistema computacional, ainda que explicando detalhadamente os procedimentos que adotará para lograr êxito.

A fase da preparação do acesso não autorizado consiste basicamente na coleta de inúmeras informações sobre o alvo. No meio técnico, esta fase é chamada de *footprinting*, pois é nela que o agente irá traçar um perfil (*footprint*)

do sistema da vítima, o que lhe possibilitará um ataque direcionado e bem sucedido[73].

> *"O footprinting de uma organização permite que invasores criem um perfil completo da postura de segurança dessa organização. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido (a conexão à Internet da Empresa X) e convertê-lo em um conjunto específico de nomes de domínio, blocos de rede e endereços IP individuais de sistemas conectados diretamente à Internet."* (MCCLURE, 2000, p. 5)

Esta é a fase de seleção da vítima. A conduta assemelha-se a de quem, em um passeio pelas ruas, procura janelas abertas para por elas furtivamente entrar. O *footprinting* evidentemente não pode ser punido, pois não há ainda qualquer ameaça concreta ao bem jurídico protegido.

Posteriormente ao *footprinting*, o agente procurará certificar quais sistemas estão ativos e alcançáveis a partir da Internet. Esta segunda fase é denominada de varredura do sistema e visa determinar principalmente as portas abertas do sistema e o sistema operacional em uso.

> *"A varredura de portas (port scanning) é o processo de se conectar a portas TCP e UDP do sistema alvo, para determinar que serviços estão em execução ou em estado de escuta. Identificar portas escutando é crucial para determinar o tipo de sistema operacional e aplicativos em*

---

[73] O agente procurará descobrir, antes dos ataques, os nomes de domínio, blocos de rede, endereços IP específicos de sistemas atingíveis via Internet, serviços TCP e UDP executados em cada sistema identificado, arquitetura do sistema (por exemplo, SPARC *versus* X86), mecanismos de controle de acesso e listas de controle de acesso (ACLs, *access control lists*) relacionadas, sistemas de detecção de intrusos (IDSs), enumeração de sistemas (nomes de usuários e de grupos, faixas de sistemas, tabelas de roteamento, informações de SNMP).

> *uso. Serviços ativos ouvindo podem permitir a um usuário não-autorizado ter acesso a sistemas mal configurados ou que estejam executando determinado software com falhas de segurança conhecidas."* (MCCLURE, 2000, p. 40-41)

Esta é a fase de avaliação da vítima. Após selecionar a vítima através do *footpriting* o pirata procurará avaliar agora a probabilidade de êxito do seu ataque. A hipótese aqui assemelha-se à de quem soa a campanhia de uma residência tão somente para saber se há pessoas no local.

Impossível também será qualquer ação contra o agente pela conduta da varredura, pois, também aqui, não há qualquer lesão ao bem jurídico protegido.

A última etapa preparatória de um acesso não autorizado consiste na identificação de contas de usuários válidas ou recursos compartilhados mal protegidos. Esta fase é chamada de enumeração.

> *"Em geral, uma vez que um nome de usuário ou de compartilhamento válido seja enumerado, normalmente é só uma questão de tempo antes que o invasor adivinhe a senha correspondente ou identifique algum ponto fraco associado ao protocolo de compartilhamento do recurso."* (MCCLURE, 2000, p. 62)

Esta é a fase da determinação das fragilidades da vítima. Assemelha-se à conduta de quem, sabendo previamente haver pessoas numa residência, procura descobrir quem são e em quais horários saem para trabalhar.

O início do ataque ao bem jurídico está aqui muito próximo, porém, não há ainda qualquer lesão concreta ao valor social tutelado. Se, por qualquer motivo, o pirata desistir de praticar o acesso não autorizado, a conduta só terá existido no âmago do agente, sem ter causado qualquer alteração real no mundo

fenomênico.

7.2. Da execução e da consumação

Vimos que o delito de acesso não autorizado a sistemas computacionais, por ser crime material, só se consumará com a ocorrência de um resultado no mundo fenomênico.

Resta-nos, no entanto, determinar quando se iniciam os atos executivos que culminam na causação deste resultado. FRAGOSO ensina que:

> *"Tendo em vista o sistema da nossa lei, prevalece na doutrina um critério objetivo de distinção, sendo irrelevante, em princípio, o plano delituoso do agente. Materialmente constitui ato de execução aquele que inicia o ataque ao bem jurídico tutelado; formalmente, tal ato distingue-se pelo início de realização da ação típica prevista pela lei."* (FRAGOSO, 1985, p. 251)

A ação de acessar dados implica em um comando que é dado pelo agente ao sistema e sua consumação se dá no momento da leitura, escrita ou execução de dados.

Este comando pode ser dado ao sistema por uma única instrução ou por uma série de instruções seqüenciais que geram o resultado final pretendido pelo agente, isto é, o acesso.

Tomemos um exemplo do cotidiano para que a hipótese seja facilmente entendida. Quando desejamos executar um programa qualquer, podemos

acessá-lo clicando duas vezes no seu ícone na área de trabalho, havendo aqui um único comando ou, no sistema operacional Windows, clicar no menu Iniciar, em seguida em programas e finalmente no nome do aplicativo a ser acessado. Neste último caso foram necessários três comandos em série para se alcançar o acesso desejado (execução do programa).

O início da execução de um acesso não autorizado dar-se-á no momento em que é emitido pelo agente o primeiro comando de uma série destinados inequivocamente a um acesso não autorizado aos dados contidos no sistema.

Como na maioria absoluta dos sistemas, o acesso a dados está protegido por senha, este primeiro comando, em geral, será uma autenticação indevida.

Como vimos, os computadores trabalham com autorizações (permissões) de acesso. O controle destas autorizações de acesso se dá por meio de um par ordenado de nome do usuário e senha.

Assim, ao ligarmos um computador ou realizarmos um acesso remoto, o sistema inicialmente nos exigirá um nome de usuário e em seguida uma senha. A máquina checará, em seguida, se o nome do usuário está armazenado em seu banco de dados e, em caso positivo, se a senha digitada corresponde àquela armazenada. Havendo a correspondência, o acesso aos dados será liberado, restando ao usuário apenas emitir os comandos desejados para que o acesso se consume.

Ao processo de conferência do par ordenado nome do usuário e senha no sistema dá-se o nome de autenticação.

Os métodos usados pelos piratas para burlarem o processo de autenticação são extremamente variados. Analisaremos aqui os principais deles, procurando determinar os exatos momentos de início de execução da conduta e de sua consumação.

7.2.1. "Engenharia social"

Os piratas denominam "engenharia social" qualquer técnica de obtenção de senhas que explore as fragilidades dos usuários e não do sistema.

Ao contrário dos demais métodos que aqui serão comentados, a "engenharia social" não requer qualquer conhecimento técnico na área de Computação, pois baseia-se tão-somente no estudo do comportamento humano.

É um fato notório que a maioria dos usuários é muito displicente na criação e na manutenção do sigilo de suas senhas. Os piratas buscam através da "engenharia social" explorar esta falha no comportamento dos usuários.

Uma das técnicas mais comuns, na tentativa de acesso por meio da "engenharia social", é o uso de dados pessoais da vítima como senha, *verbi gratia* sua data de nascimento. Parece incrível, mas muitos usuários utilizam-se de seus sobrenomes e dos nomes das esposas, namoradas e filhos como senhas, o que evidentemente serão as primeiras opções a serem tentadas por um invasor.

Uma outra técnica de "engenharia social" bastante difundida consiste

simplesmente em perguntar à vítima qual é a sua senha, induzindo esta a erro, mediante meio fraudulento.

O famoso *hacker* Kevin Mitnick conseguiu inúmeras senhas de sistemas ligando para empresas e se fazendo passar por um técnico do Departamento de Informática. As vítimas inocentemente ditavam suas senhas na crença de se tratar de pessoa autorizada. Esta técnica também foi bastante explorada pelo lendário *hacker* norte-americano para traçar o *footprint* de muitos sistemas por ele invadido.

Em páginas da Internet que oferecem serviços gratuitos de emails é comum os piratas registrarem emails que aparentam ser do setor de suporte da página como: suporte@emailgratuito.com.br; duvidas@emailgratuito.com.br ; ajuda@emailgratuito.com.br; recadastramento@emailgratuito.com.br e outros. Em seguida enviam mensagens através destes emails aos usuários cadastrados no sistema afirmando que suas senhas deverão ser trocadas e requisistando que seja enviada uma resposta para aquele email com a senha antiga e a senha nova. A porcentagem de sucessos em ações como essa é muito significativa.

As técnicas de "engenharia social" são inúmeras, porém, interessa-nos aqui determinar tão somente quando se caracteriza o início da execução do acesso não autorizado.

Em tais hipóteses, a execução do acesso não autorizado só se iniciará quando o usuário tentar autenticar-se no sistema usando a senha obtida pela "engenharia social". As fases anteriores são meramente preparatórias, pois o

pirata pode obter as senhas por meio da "engenharia social" sem, no entanto, jamais tentar acessar o sistema da vítima, o que não constitui sequer uma ameaça real aos dados protegidos.

Em uma analogia com o crime de homicídio, podemos dizer que o agente comprou a arma, mas ainda não mirou e muito menos apertou o gatilho.

Vale ressaltar que a engenharia social é uma técnica de obtenção de senhas que pode ser utilizada tanto em acessos locais como em acessos remotos.

7.2.2. Ataques de força bruta

A autenticação em um sistema baseia-se na conferência de um par ordenado de nome-do-usuário e senha que é digitado no momento da inicialização e aquele armazenado no banco de dados do sistema. Havendo a exata correspondência o acesso ao sistema é liberado, caso contrário é possível uma nova tentativa.

Os ataques de força-bruta baseiam-se nesta fragilidade do sistema, buscando, por uma seqüência de tentativa e erro, encontrar o par ordenado nome-do-usuário/senha capaz de liberar o sistema.

Em tese, esta operação poderia ser realizada manualmente, mas é evidente que seria necessária grande disposição e disponibilidade de tempo do agente para que obtivesse êxito na empreitada.

Os piratas criam então programas que automatizam a tarefa de, por tentativa e erro, testar cada um dos pares ordenados que eles supõem ser prováveis de liberar o acesso.

Tais programas trabalham com dois dicionários: um com prováveis nomes-de-usuários, outro com senhas comuns. Como exemplos de nomes-de-usuários comuns podemos citar: maria, joao, pedro, marcelo, tulio ou qualquer outro prenome usual na língua portuguesa. Exemplos de senhas usuais são todas as datas de nascimento próximas à faixa etária do usuário, a mesma lista de nomes (pois nomes próprios são comuns em senhas) e nomes de artistas famosos.

É comum ainda o uso de dicionários específicos com palavras relacionadas ao conteúdo armazenado no sistema. *Verbi gratia*, se se tenta invadir um sistema de um escritório de advocacia, usa-se um dicionário de termos jurídicos, se a intenção é acessar uma clínica médica, o dicionário será de termos próprios da medicina e, os casos mais freqüentes, se se deseja o acesso a um sistema com conteúdo pornográfico, o dicionário será formado por palavras de baixo calão.

O início da execução do delito se dá com a liberação do acesso, mas o crime só se consumará caso algum dos dados armazenados no sistema seja efetivamente acessado (via leitura, escrita ou execução).

Assim como a engenharia social, os ataques por meio de tentativa e erro (força bruta) podem ser usados tanto em acessos locais como em acessos remotos.

7.2.3. Acesso local (*off line*)

O acesso local é aquele em que o agente tem contato físico com o computador que acessa, emitindo seus comandos através de um dispositivo de entrada de dados (teclado, mouse, etc) diretamente conectado ao computador acessado.

Pode se dar às escondidas, ou mesmo, mediante violência ou grave ameaça à pessoa[74].

Os sistemas computacionais são bastante vulneráveis a acessos físicos e há muito pouco que se possa fazer para protegê-los nestes casos, a não ser trancar as máquinas em um cofre.

As senhas da BIOS[75] podem ser apagadas retirando-se a bateria da placa-mãe. Nestes casos o acesso se iniciará no momento em que a senha for apagada, mas só se consumará no momento em que algum dado for lido, escrito ou executado.

A subtração do disco rígido no qual os dados estão armazenados, para a leitura posterior em outro sistema, constituirá o crime de furto, podendo este ser absorvido pelo acesso não autorizado caso o acesso se consume

---

[74] Cf. o art. 615 ter, 2, do *Codice penale* italiano: *"se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato."* Disponível em: <http://www.studiocelentano.it/cp/codicepenale000.htm>.

[75] Cf. nota 58 na p. 78.

posteriormente, pois neste caso o furto será crime-meio.

Há que se levar em conta, evidentemente, nestas circunstâncias, o dolo do agente. Se sua intenção era subtrair o disco rígido pelo valor patrimonial que o dispositivo tem mesmo quando formatado, haverá furto; se porém, buscava o conteúdo armazenado no disco, istó é, os dados, haverá acesso não autorizado a sistema computacionais, sendo o furto crime-meio não apenado com base no princípio da consunção.

7.2.4. Acesso remoto (*on line*)

O acesso remoto é o método mais comum de invasão de sistemas computacionais. Não há qualquer contato físico do pirata com o computador invadido e o computador no qual o agente emite os comandos de acesso é diferente daquele em que os dados estão armazenados. O acesso se dá através de uma rede que, na maioria absoluta das vezes, é a Internet.

As técnicas da acesso remoto são extremamente diversificadas e sua enumeração exaustiva certamente excederia os limites deste trabalho. Variam de acordo com o sistema operacional da vítima e, em sua grande maioria, procuram explorar *bugs*[76] ou a má configuração do sistema operacional e dos

---

[76] Do inglês – inseto. Designa erros de programação. A origem do vocábulo é curiosa: *"A palavrinha já vinha sendo usada como gíria para significar complicação desde os primórdios da Revolução Industrial. No século XIX, quando as máquinas começaram a substituir o trabalho braçal, elas foram instaladas em galpões abertos, onde havia uma variada frota de insetos*

aplicativos instalados.

Em todos os casos, no entanto, haverá duas fases bem distintas: a emissão do comando (ou da seqüência de comandos) pelo agente a partir de seu computador e o resultado fático de sua conduta, qual seja, o acesso não autorizado em uma de suas modalidades (leitura, escrita ou execução).

7.2.5. Cavalo-de-tróia[77]

Os cavalos-de-tróia (*Trojan horses*) são pequenos programas, muito semelhantes aos vírus, que infectam sistemas computacionais, permitindo que

---

voando para lá e para cá, o tempo todo. A possibilidade de um deles pousar no lugar errado e causar estragos era grande, e aí qualquer parada mecânica era, em princípio, atribuída a um bug. Só que no caso dos computadores foi um bug de verdade: sabe-se lá como, uma mariposa conseguiu entrar num Mark II do Centro Naval de Virgínia, nos Estados Unidos, e travou todo o sistema. O episódio aconteceu em 1945, e está perfeito e hilariamente documentado, porque o técnico que descobriu a mariposa a anexou a seu Relatório de Manutenção, grudando a danadinha com fita adesiva, após explicar tecnicamente: Havia um bug no sistema. Daí em diante, o nome passaria a ser sinônimo de qualquer tipo de falha ou erro, sendo que o mais famoso (e mais caro) de todos os bugs foi o bug do milênio, que iria paralisar o mundo na virada de 1999 para 2000. Calcula-se que, para neutralizá-lo, foram gastos 120 bilhões de dólares, dinheiro suficiente para comprar todo o estoque de inseticidas do mundo!" (GEHRINGER et LONDON, 2001, p.21)

[77] O nome do programa é uma referência ao mitológico Cavalo de Tróia, que aparece no episódio do Laocoonte, uma das passagens da *Eneida* de Virgílio: *"Fatigados por um cerco e uma série de combates que havia dez anos duravam, os gregos recorreram a um estratagema para penetrar em Tróia, tão bem defendida. Construíram, segundo as lições de Palas-Minerva, um enorme cavalo, com tábuas de pinheiro, artisticamente unidas no conjunto, e fizeram correr a notícia de que era uma oferta que consagravam àquela deusa, para obter um feliz regresso à pátria. Encheram de soldados os flancos desse enorme cavalo, e fingiram que se afastavam. Os troianos, vendo esse colosso sob seus muros, resolveram apoderar-se dele e colocá-lo na cidadela. (...) Os troianos fazem entrar na cidade o colosso fatal e colocam-no no templo de Minerva. Na noite seguinte, enquanto toda a cidade estava mergulhada em profundo sono, um traidor, trânsfuga do exército grego, chamado Sinon, abre os flancos do cavalo, deixa uma saída aos soldados, e então Tróia é tomada e entregue às chamas."* (COMMELIN, p. 238)

piratas os acessem remotamente, em geral, através da Internet.

O agente oferece à vítima um programa para que ela o execute em seu computador (geralmente são enviados por email ou são postados em grupos de discussão). Este programa pode vir disfarçado como um jogo ou como qualquer outro executável, que funciona perfeitamente, mas que posssui embutido em seu código instruções de controle remoto do sistema.

Assim, ao executá-lo, a vítima cria uma conexão direta do seu sistema com o computador do pirata, que pode ler, modificar, apagar ou inserir dados no computador da vítima com facilidade. Também é possível, através dos cavalos-de-tróia, reinicializar o sistema, abrir e fechar o compartimento do CD-ROM, conversar com a vítima por uma tela de *chat* ou mesmo ver sua fisionomia se houver uma Web Cam instalada no sistema. E, claro, ler todas as senhas e arquivos da vítima armazenadas no sistema e transferí-los para outro computador.

O acesso obtido através de um cavalo-de-tróia só se compara àqueles obtidos localmente, tamanho é o controle do sistema pelo invasor. Sua prevenção se faz através de programas antivírus atualizados.

O início da execução se dá no momento da divulgação do programa, mas o crime só se consumará quando o pirata acessar quaisquer dos dados armazenados no sistema da vítima.

7.3. Tentativa

A tentativa de acesso não autorizado a sistemas computacionais se configurará todas as vezes em que, após emitido o comando ou a seqüência de comandos que visem dar causa ao acesso, este não ocorrer por motivos alheios à vontade do agente.

Assim, se após iniciada a execução, o agente não conseguir ler (e compreender), alterar ou executar os dados, por circunstâncias alheias à sua vontade, o delito será punido em sua modalidade tentado.

A leitura dos dados tem como resultado a sua compreensão. Estando os dados em idioma estrangeiro não compreensível pelo agente ou, ainda, criptografados, haverá crime impossível[78].

A escrita de dados tem como resultado a sua alteração. Assim, se o agente modifica o arquivo, mas logo em seguida, arrependido, restaura o *status quo ante*, haverá o arrependimento eficaz previsto no art. 15 do Código Penal Brasileiro.

O processamento de dados tem como resultado a execução do programa. Assim, se o agente ordena a execução do programa, mas este por um

---

[78] A este respeito tome-se a lição de FRAGOSO comentando o crime de violação de correspondência: *"A mensagem cifrada ou a carta em língua estrangeira, que o agente não consegue traduzir, são objetos inadequados para a tentativa, que se configurará, porém, quando o agente abre o envelope e, por circunstâncias alheias à sua vontade, não chega a ler a correspondência."* (FRAGOSO, 1983. p.231). Obviamente nas modalidades de escrever e processar dados o crime será perfeitamente possível.

problema interno qualquer, retorna uma mensagem de erro, haverá crime impossível por absoluta impropriedade do objeto e o agente não será punido, por expressa disposição do art. 17 do Código Penal Nacional.

8. DOS SUJEITOS DO DELITO

8.1. Sujeitos ativo e passivo

O sujeito passivo do delito de acesso não autorizado a computadores será qualquer pessoa física ou jurídica proprietária dos dados armazenados no sistema.

O sujeito ativo será a pessoa humana responsável pela emissão do comando causador da leitura, escrita ou execução de dados para os quais não tinha autorização.

Nada impede que o empregador seja sujeito ativo quando acessar os emails ou arquivos pessoais do empregado armazenados no sistema computacional. O fato de o empregador ser o proprietário do sistema não o isentará do crime, pois o que se protege no delito de acesso não autorizado é a inviolabilidade dos dados informáticos e estes são de propriedade do empregado.

Se não é do interesse do empregador que o empregado mantenha arquivos pessoais em seu sistema, deverá notificá-lo para que ele os exclua de lá, mas jamais acessar os dados do empregado à sua revelia, pois isto caracterizará o acesso não autorizado.

Poderá ser sujeito ativo do delito ainda o cônjuge que acesse os dados do outro sem sua autorização, pois a proteção constitucional (art. 5º, X) garante a intimidade e a vida privada, direitos individuais do cidadão que são a essência

da tutela penal à inviolabilidade dos dados informáticos.

O casamento não elimina dos cônjuges seu direito individual à privacidade, pois há em cada indíviduo uma necessidade natural de manter determinados segredos só para si. Assim, se um cônjuge acessa sem autorização os dados informáticos do outro, estará cometendo acesso não autorizado a sistemas computacionais, pois a lesão ao bem jurídico privacidade individual é evidente.

A União, os Estados, o Distrito Federal e o Município, quando sujeitos passivos do acesso não autorizado a computadores, deverão ter uma proteção penal maior, pois a ofensa à integridade de seus dados não lesa um indíviduo somente, mas toda a comunidade, razão pela qual o crime deverá ser qualificado quando estes forem seus sujeitos passivos.

Determinados agentes terão maior facilidade para obterem o acesso não autorizado aos sistemas, como o caso dos administradores de sistemas, que possuem meios técnicos para acessarem os dados, e os funcionários públicos responsáveis pelo processamento de inúmeros dados sigilosos. A estes certamente deverá ser cominada pena mais severa quando, em razão de seus cargos, obtiverem o acesso não autorizado.

8.2. Responsabilidade penal da pessoa jurídica

A maioria dos programas disponíveis no mercado são distribuídos com o código fechado, o que impede que mesmo programadores de alto nível possam

saber ao certo quais instruções são processadas no sistema do usuário.

Se uma empresa, desenvolvedora de *softwares*, elabora e distribui um programa – um editor de textos, por exemplo – que ao ser instalado no computador do usuário realize não só as funções para as quais foi adquirido, mas, também, envie através da Internet à empresa desenvolvedora quaisquer dados armazenados no computador da vítima – como por exemplo, nome, endereço, telefone, ou mesmo senhas – sem o conhecimento do usuário, estaremos diante de um típico caso de acesso não autorizado a sistemas computacionais.

A responsabilidade penal da pessoa jurídica desenvolvedora de programas que, quando executados no computador da vítima, permitem um acesso não autorizado a seu sistema, é discutível.

No passado já se puniu penalmente os animais e hoje tal fato nos parece ridículo. Contudo, paradoxalmente, não nos parece ridículo punir penalmente uma empresa.

Animais efetivamente realizam ações (obviamente não há culpabilidade neles, mas estamos tratando de ação). Animais andam, correm, matam... Empresas, no entanto, não têm como realizar ações, salvo por metonímia[79].

---

[79] *[Do gr. metonymía, pelo lat. metonymia.] S. f. E. Ling. 1. Tropo que consiste em designar um objeto por palavra designativa doutro objeto que tem com o primeiro uma relação de causa e efeito (trabalho, por obra), de continente e conteúdo (copo, por bebida), lugar e produto (porto, por vinho do Porto), matéria e objeto (bronze, por estatueta de bronze), abstrato e concreto (bandeira, por pátria), autor e obra (um Camões, por um livro de Camões), a parte pelo todo*

Afirmar que uma empresa acessou sem autorização um sistema computacional é tranferir a responsabilidade penal do responsável pelo programa para a empresa para a qual trabalha.

Não é crível imaginarmos todos os funcionários desta empresa, incluindo aí seus administradores, programadores, gerentes de vendas, contadores e funcionários dos serviços-gerais, acessando indevidamente um sistema computacional.

A transferência da responsabilidade penal para a pessoa jurídica acabaria ferindo diretamente a garantia constitucional de que nenhuma pena passará da pessoa do condenado, pois uma pena de suspensão de atividades, por exemplo, certamente geraria prejuízos para os funcionários que em nada contribuíram para a realização do crime. A punição estender-se-ia do diretor ao porteiro, o primeiro muita vez culpado, o segundo na grande maioria das vezes, completamente inocente.

Além do mais, partindo-se de um conceito ontológico de conduta, é mais fácil admitir que um cão poluiu um rio do que uma empresa, pois o animal pode perfeitamente carregar um objeto em sua boca e jogá-lo no rio, mas uma empresa, salvo por metonímia, jamais poderia praticar uma ação destas.

A este respeito, ZAFFARONI et PIERANGELI ensinam que:

(asa, por avião), etc. (FERREIRA, 1999)

> *"Não se pode falar de uma vontade em sentido psicológico no ato da pessoa jurídica, o que exclui qualquer possibilidade de admitir a existência de uma conduta humana. A pessoa jurídica não pode ser autora de delito, porque não tem capacidade de conduta no seu sentido ôntico-ontológico."* (ZAFFARONI et PIERANGELI, 1999. p. 410)

Se admitíssemos a responsabilidade penal da pessoa jurídica, estaríamos nos afastando do princípio do *nullum crimen sine conducta*, pois pessoa jurídica não realiza conduta alguma. Num estado democrático de direito não se pode admitir tal hipótese. O que pode e deve haver é responsabilidade civil ou administrativa, jamais penal.

Argumentam os defensores da responsabilidade penal da pessoa jurídica que a Constituição Federal de 1988 expressamente previu tal possibilidade em seu art. 225 § 3º ao estabelecer que:

> *"as condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados."*

Reescrita a frase de outro modo, temos: As condutas sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas.

Pessoas físicas ou jurídicas é um aposto explicativo do objeto direto infratores e pode ser retirado da frase sem alterar-lhe o sentido. Sua única função na frase é explicitar quem pode ser infrator, mas o objeto indireto **a sanções penais e administrativas** não lhe tem qualquer relação.

A conjunção **e** é aditiva e indica que os infratores deverão sofrer ambas as

sanções constantes do objeto indireto: penal e administrativa.

Assim, pela simples interpretação gramatical do dispositivo constitucional, chega-se à conclusão de que a Constituição admite a possibilidade teórica de uma sanção penal de uma pessoa jurídica.

Da mesma forma, poderia a Carta Magna ter admitido a responsabilidade penal das armas utilizadas em homicídios. Só há um porém. Empresas, assim como armas, não realizam ações típicas; não são sujeitos.

Na frase "A espada matou Tício" está clara a metonímia. Substituiu-se a causa ativa pelo instrumento. Melhor seria dizer "Mévio matou Tício com sua espada", em que espada seria adjunto adverbial de instrumento.

Da mesma forma na frase A empresa poluiu o rio, melhor seria dizer Caio poluiu o rio com sua empresa. Empresa é, pois, adjunto adverbial de instrumento, jamais sujeito.

Querer punir a empresa de Caio é o mesmo que querer punir a espada de Mévio. É querer punir o instrumento do crime e não seu sujeito.

A previsão teórica da Constituição admitindo a responsabilidade penal da pessoa jurídica é dispositivo sem qualquer aplicação prática, pois pessoa jurídica alguma jamais praticará efetivamente qualquer ação típica[80].

---

[80] Sobre a responsabilidade penal da pessoa jurídica cf. SALES, Sheila Jorge Selim de. *Do sujeito ativo:* na parte especial do Código Penal. Belo Horizonte: Del Rey, 1993. e PRADO, Luís Regis. *Curso de Direito Penal Brasileiro*: parte geral. 2.ed. rev., atual. e ampl. São Paulo:

Pelo exposto, entendemos que, nos casos de acessos não autorizados a computadores oriundos de programas desenvolvido por pessoas jurídicas, a responsabilidade penal será dos diretores da empresa e da equipe de programadores responsável pelo programa e deverá ser analisada caso a caso, devendo cada um deles ser punido na medida de sua culpabilidade, sem exclusão, evidentemente de sanções administrativas para a empresa.

8.3. Concurso de agentes

O acesso não autorizado a sistemas computacionais pode ser realizado por uma ou mais pessoas. Neste último caso, estaremos diante de uma hipótese de concurso de agentes.

Antes de iniciarmos o estudo do concurso de agentes no acesso não autorizado a sistemas computacionais, convém que nos detenhamos na análise da existência e da relevância da distinção entre co-autoria e participação.

O art. 29 do Código Penal Brasileiro estabelece que:

> *"Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida da sua culpabilidade."*

Editora Revista dos Tribunais, 2000.

Aparentemente poder-se-ia imaginar que nosso código adotou uma concepção extensiva de autor, baseado na eficiência causal. Assim, seria autor todo o indivíduo que desse causa ao crime.

O fato de a lei não distinguir entre autoria e participação não pode, no entanto, servir de argumento para afirmar que, em nosso ordenamento jurídico-penal, não haja esta distinção.

Ocorre que não cabe ao legislador diferenciar a autoria da participação, pois estes são conceitos ônticos. A esse respeito ZAFFARONI e PIERANGELI fazem a seguinte analogia:

> *"Ocorre algo análogo quando se organiza um baile: as entradas podem ter preços diferentes para os homens e para as damas, mas nada impede que tenham o mesmo preço. Os organizadores limitam-se a estabelecer o preço das entradas para os que acorrerem ao baile, que pode ser igual, ou diferente, para cavalheiros e damas, mas os organizadores do baile não se ocupam de definir homens e mulheres, porque estes são dados ônticos."* (ZAFFARONI et PIERANGELI, 1999. p. 665)

A doutrina, partindo de uma concepção restritiva de autor, procurou distinguir a autoria da participação[81]. Surgiram então diversas teorias que procuram diferenciá-las a partir de uma série de critérios.

O critério subjetivo deriva da concepção extensiva de autoria, que tem como base a teoria da *conditio sine qua non*. Por este critério, o que distingue autor

---

[81] A palavra participação aqui será empregada no seu sentido estrito, pois, em rigor, o autor também participa do crime.

de partícipe é que o primeiro deseja praticar o crime como próprio, atuando com vontade de autor (*animus auctoris*) enquanto o segundo não. A fragilidade deste critério é visível, pois despreza completamente os elementos objetivos da conduta e, evidentemente, ele não teve maior repercussão em nosso sistema jurídico.

A concepção material-objetiva surge com a teoria da "causa eficiente" ou "teoria da eficiência" e diferencia causa de condição. Segundo esta concepção, a causa não é qualquer antecedente, mas a condição mais eficaz, que busca revelar as diferenças materiais entre as ações dos diversos concorrentes. Autor é aquele cuja conduta dá causa ao evento; partícipe é aquele que, para a produção do resultado, coloca apenas condições. Esta concepção não foi acatada por nosso ordenamento jurídico, já que nosso Código Penal adota expressamente a teoria unificadora dos antecedentes, a da *conditio sine qua non*, dispondo em seu art. 13:

> *"(...) Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido."*

A concepção formal-objetiva é assim denominada por acentuar as características exteriores ou formais da conduta, em sua conformação com o tipo penal. Por esse critério, só pode ser autor aquele que realiza pessoalmente toda a ação descrita no tipo. O partícipe é aquele que colabora de qualquer forma para a realização de uma conduta típica de outrem. Assim, a conduta do partícipe por si só não é típica. Esta teoria, de inspiração causalista, é adotada por vários autores nacionais.

A teoria do "domínio do fato", de inspiração finalista, não exige para a configuração da autoria a realização direta ou de própria mão do delito. Segundo esta teoria é autor quem tem domínio do fato. Aquele que tem poder de decisão sobre a configuração central do fato. Esta teoria também teve larga aceitação na doutrina nacional.[82]

Vistos os principais posicionamentos doutrinários sobre o tema, analisaremos o concurso de agentes no delito de acesso não autorizado a sistemas computacionais, procurando demonstrar as hipóteses tanto com base no critério formal-objetivo, quanto na teoria do "domínio do fato".

Suponhamos uma hipótese em que duas pessoas, de comum acordo e utilizando-se de um único computador, obtêm acesso sem autorização a um sistema computacional. Um dos agentes, pirata experiente, dita os procedimentos para um neófito em informática desejoso de aprender as técnicas da criminalidade informática, acessando ambos, sem autorização, um sistema computacional.

O núcleo da conduta típica de um acesso não autorizado seria a própria ação de acessar que, como foi dito, pode se dar na modalidade de leitura, escrita ou processamento de dados. A execução dos comandos se dá, em geral, por meio de um teclado.

---

[82] Sobre os diversos critérios de distinção entre autoria e participação cf. RAMOS, Beatriz Vargas. *Do concurso de pessoas*: contribuição ao estudo do tema na nova parte geral do código penal. Belo Horizonte: Del Rey, 1996.

Adotando-se o critério formal-objetivo, conclui-se que somente quem digita os comandos no teclado pode ser considerado autor, pois é quem executa pessoalmente a conduta típica de emitir os comandos necessários ao computador para que o acesso seja concretizado. Aquele que a seu lado o orienta, auxilia ou mesmo lhe dita as instruções necessárias para se obter o acesso seria considerado simplesemente como partícipe.

Esta não parece ser uma solução adequada, pois, em determinadas situações concretas, seria como considerar autor de um livro seu digitador e não aquele que ditou seu conteúdo.

A "teoria do domínio do fato" melhor soluciona a hipótese. Segundo esta teoria, será autor do acesso não autorizado aquele que tiver o domínio do fato.

Na hipótese do pirata que dita os comandos necessários para o êxito do acesso ao aprendiz, ambos serão co-autores do delito, ainda que o pirata não tenha emitido pessoalmente o comando responsável pela invasão.

Na hipótese acima tratada, o concurso de agentes foi realizado com ambos os autores em um mesmo local físico e utilizando-se de um único sistema computacional para praticarem a conduta.

Ao concurso de agentes no qual estes utilizam-se de um único sistema computacional para realizarem o ataque denominaremos de unilateral, em oposição àquele em que os agentes utilizarem dois ou mais sistemas computacionais conectados em rede para realizarem o ataque, ao qual chamaremos de plurilateral.

Esta última é a hipótese mais comum de concursos de agentes nos delitos informáticos e já existem, inclusive, inúmeros grupos na Internet que têm por objetivo a invasão de sistemas computacionais.

A maioria nunca se viu pessoalmente e reside em cidades diferentes, comunicando-se tão somente por meio da Internet.

No momento do ataque, cada um dos agentes, de comum acordo com os demais, emite em seu computador comandos que dão causa ao acesso não autorizado no sistema da vítima.

Por fim, vale lembrar que em todo concurso de agentes, deverá haver acordo de vontades consciente entre os autores para a prática do delito, sendo impensável considerar autor de um acesso não autorizado alguém que simplesmente escreveu um livro ensinando técnicas de invasão ou que tenha desenvolvido um programa de computador para este fim.

9. CONCLUSÕES

Apresentamos as conclusões de nosso estudo em duas partes.

Na primeira, nossa proposta de tipificação do acesso não autorizado a sistemas computacionais no ordenamento jurídico brasileiro.

Na segunda, os comentários resumidos acerca do novo tipo penal, com base em tudo o que foi tratado no corpo do texto.

9.1. De lege ferenda

O Congresso Nacional Decreta:

Art. 1º O Decreto-Lei nº 2.848 de 7 de dezembro de 1940 – Código Penal – passa a vigorar acrescido em sua Parte Especial, Título I, Capítulo VI, da seguinte Seção V:

Seção V – Dos crimes contra a inviolabilidade de dados informáticos

Acesso não autorizado a sistemas computacionais

Art. 154-A. Acessar, sem autorização, dados ou programas em sistema computacional.

Pena – prestação de serviços à comunidade ou a entidades públicas, de 1 (um) a 2 (dois) anos e multa.

§ 1º. A pena será reduzida de um a dois terços ou o juiz aplicará somente a pena de multa se o agente não tinha intenção de lucro ou de obter vantagem de qualquer espécie para si ou para outrem e foi pequeno o prejuízo para a vítima.

§ 2º. Aumenta-se a pena de um terço até metade:

I – se o crime é cometido contra sistema computacional da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – se o crime é cometido por funcionário público ou por quem exerça a função de administrador de sistemas ou assemelhada, com abuso de poder ou com violação de dever inerente a função;

III – se o agente destrói ou danifica o sistema computacional ou os dados nele armazenados;

IV – se o agente divulga a terceiros as informações obtidas, causando dano material ou moral à vítima.

§ 3º. A pena prevista neste artigo será cumprida preferencialmente por meio de tarefas que aproveitem as aptidões do condenado, especialmente no desenvolvimento de softwares com código aberto para entidades públicas e no treinamento em informática de funcionários públicos e da comunidade em geral.

§ 4º. Somente se procede mediante representação, salvo na hipótese do § 2º,

II, em que a ação é pública incondicionada.

Art. 2º Fica inserido ainda no mesmo Código o seguinte art. 44-A:

Art. 44-A. As penas restritivas de direitos são autônomas e principais quando expressamente cominadas no tipo legal e serão calculadas nos termos do art. 68 deste Código.

Parágrafo Único. Em caso de descumprimento injustificado da restrição imposta, aplica-se o disposto no § 4º do art. 44.

Art. 3º O *caput* do art. 45 passa a ter a seguinte redação:

Art. 45. Na aplicação das penas restritivas de direitos, proceder-se-á na forma deste e dos arts. 46, 47 e 48.

Art. 4º Esta lei entra em vigor na data de sua publicação.

9.2. Comentários

9.2.1. Bem jurídico tutelado

O bem jurídico penalmente tutelado é a inviolabilidade dos dados informáticos.

A inviolabilidade compreende não só o direito à privacidade e ao sigilo dos dados, como também à integridade destes e sua proteção contra qualquer destruição ou mesmo alteração.

Dados informáticos são as informações representadas em forma apropriada para armazenamento e processamento por computadores.

Os programas são considerados dados *lato sensu* e se diferem dos dados *stricto sensu* por serem séries de instruções que podem ser executadas pelo computador para se alcançar um resultado pretendido, mas também são objeto de proteção da norma.

9.2.2. Sujeitos do delito

O sujeito ativo é qualquer pessoa humana não autorizada a acessar os dados.

O proprietário do sistema computacional, o empregador e o cônjuge poderão ser sujeitos ativos se não possuírem autorização para acessar os dados.

Sujeito passivo é qualquer pessoa, física ou jurídica, proprietária dos dados informáticos.

9.2.3. Tipo objetivo

O verbo típico é **acessar** e deve ser entendido como a ação de ler, escrever ou executar dados armazenados em sistemas computacionais.

A leitura é a recuperação dos dados armazenados no sistema com sua conseqüente interpretação como informações humanamente inteligíveis. A

escrita consiste na inserção, remoção ou alteração de dados no sistema. A execução de dados, mais precisamente de programas, é o processamento de informações automatizadas de acordo com instruções pré-estabelecidas.

O objeto material do delito são os dados informáticos, isto é, os dados *stricto sensu* e os programas de computadores.

O conceito normativo de autorização não se confunde com o conceito de autorização da Ciência da Computação, pois neste a autorização é entendida como os atributos que controlam o acesso a arquivos e diretórios de um sistema computacional e naquele como a relação de legitimidade de um sujeito para acessar dados em um sistema computacional.

Sistema computacional é um conjunto de dispositivos interconectados capaz de processar dados automaticamente.

9.2.4. Tipo subjetivo

É o dolo, ou seja, a vontade livre e consciente de acessar sem autorização dados ou programas em sistema computacional.

Na escola tradicional é o "dolo genérico".

Inexiste modalidade culposa.

9.2.5. Tempo e local do delito

O art. 4º do Código Penal Brasileiro adota para a fixação do momento do delito a teoria da atividade. Assim, o acesso não autorizado a computadores será considerado realizado no momento em que foi emitido o comando ou a seqüência de comandos, destinados inequivocamente a causar um acesso não autorizado aos dados de um sistema computacional.

O art. 6º do Código Penal Brasileiro adota para a fixação do local do delito a teoria da ubiqüidade, assim o acesso não autorizado a computadores será considerado praticado tanto no local da execução quanto no local da consumação.

Se forem distintos os países onde se deram a execução e a consumação do delito, para que o agente possa ser punido é necessário que a conduta seja típica em ambos os países.

9.2.6. Consumação e tentativa

Trata-se de crime material e, como tal, exige um resultado no mundo fenomênico para que ocorra a tipicidade da conduta.

O crime se consuma com a leitura, escrita ou execução dos dados do sistema computacional.

É admissível a tentativa quando, após iniciada a execução, o crime não se

consuma por circunstância alheia à vontade do agente.

Se os dados acessados indevidamente estiverem criptografados, o crime será impossível.

Se o agente, após modificar os dados do sistema, arrepender-se e restaurar o *status quo ante*, haverá o arrependimento eficaz.

9.2.7. Concurso de crimes

Quando o acesso não autorizado a computadores for crime-meio para a prática de outro delito, não será punido, e o delito-fim será denominado de crime informático mediato ou indireto.

9.2.8. Concurso de agentes

É perfeitamente possível a co-autoria e a participação.

O concurso de agentes será unilateral ou plurilateral. Unilateral quando todos os agentes utilizarem-se de um único sistema computacional para realizarem o ataque. Plurilateral quando os agentes utilizarem dois ou mais sistemas computacionais conectados em rede para realizarem o ataque.

Para a teoria formal-objetiva será autor quem emitir o comando ou a seqüência de comandos que der causa ao acesso não autorizado. Aquele que o auxiliar

ditando os procedimentos necessários para lograrem êxito será partícipe.

Para a teoria do "domínio do fato" ambos serão co-autores do acesso não autorizado e responderão na medida de sua culpabilidade.

9.2.9. Competência

Quando praticados na Internet, deverão ser conhecidos e julgados pela Justiça Federal, uma vez que a Internet é um serviço público da União.

A competência será da Justiça Comum, quando o agente não se utilizar da Internet para obter o acesso não autorizado ao sistema computacional.

9.2.10. Ação penal

A ação penal é pública condicionada a representação exceto quando cometida contra o Estado, caso em que será pública incondicionada.

O titular do direito de representação será o proprietário dos dados.

9.2.11. Causa de diminuição de pena

São dois os requisitos para a aplicação da causa de diminuição de pena prevista no § 1º: 1) ausência de ânimo do agente de obter lucro ou vantagem

de qualquer espécie para si ou para outrem, podendo ter cometido o crime com *animus jocandi* ou por simples curiosidade. 2) *pequeno prejuízo para a vítima*, que melhor deverá ser interpretado como valores abaixo de um salário mínimo vigente à época dos fatos.

9.2.12. Causa de aumento de pena

O delito é punido com maior rigor quando cometido contra sistema computacional da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos, pois, sendo os dados de interesse público, justifica-se uma tutela mais rigorosa do bem jurídico.

A pena também será aumentada quando o agente abusar de sua função de funcionário público ou de administrador de sistemas em razão de seu cargo, pois aqui a culpabilidade do agente é maior, já que era seu dever velar pela inviolabilidade dos dados informáticos.

O dano causado ao sistema computacional ou aos dados, bem como a divulgação a terceiros das informações obtidas com dano moral ou material à vítima também é causa de aumento de pena, por sua maior lesividade ao bem jurídico tutelado.

POST SCRIPTUM – DAS PENAS

No princípio era o delito:

Artigo Único – Comer a maçã.

Pena: expulsão do Paraíso.

Parágrafo Único- Na mesma pena incorre quem, de qualquer modo, concorre para este crime.

A Bíblia não nos narra os fatos nestes termos. Talvez porque algum copista, incomodado com tamanho predomínio do Direito Penal, a tenha reescrito de forma mais branda.

Quando Gutemberg imprimiu o primeiro exemplar da Bíblia, possivelmente não imaginou a revolução que seu invento causaria. A imprensa proporcionou ao homem não só a preservação de sua cultura, mas também sua difusão de uma forma jamais anteriormente imaginada.

A Internet e, por extensão, toda a informática, é a reinvenção da imprensa. Alguém com um computador ligado à Internet tem praticamente toda a cultura humana disponível a um clicar de *mouse*.

Mas a Internet não se limitou a reinventar a imprensa. Reinventou também a moeda e o cheque; o cavalo, a locomotiva e o telégrafo; o disco de vinil, a fita K7 e o CD; o VHS e a TV; a amizade e o namoro. Talvez a democracia; provavelmente o trabalho; com toda certeza as relações contratuais. E, claro, o

crime... a Internet, porém, não reinventou o cárcere.

O ser humano que pisou na Lua, clonou animais e foi capaz de criar um verdadeiro universo virtual ainda trava guerras, morre de subnutrição e encarcera criminosos.

O grande desenvolvimento das ciências naturais parece não ter sido acompanhado em igual proporção pelas ciências sociais. O Direito Penal, que sofreu significativas mudanças em sua Teoria do Delito, não parece ter solucionado ainda seu grande dilema: como punir?

A solução para esta questão foge completamente ao objeto de estudo desta dissertação, que procurou examinar a matéria exclusivamente com base na Teoria do Crime. O que se buscou aqui foi analisar o tipo penal de acesso não autorizado a sistemas computacionais a fim de se fornecer subsídios para legisladores e aplicadores da norma penal.

Não foi nosso objetivo adentrar pelos meandros da Teoria da Pena e, muito menos, definir qual pena seria a mais adequada para a punição deste delito. Nossa proposta foi responder a indagação: o que é o acesso não autorizado a sistemas computacionais? e não: como puní-lo? A resposta à segunda questão, por si só, ensejaria um novo trabalho.

Uma breve observação, no entanto, se faz necessária.

Em tempos de Direito Penal mínimo, quando sonhamos com uma Parte Especial de Código Penal que possa ser impressa em uma única lauda de papel A4, é no mínimo paradoxal que proponhamos a criminalização de novas

condutas, num ordenamento jurídico com centenas de tipos em vigor.

Se impossível deixar de fazê-lo hoje, no estado atual de nossa ciência, ao menos que busquemos formas mais dignas e eficazes ou, por que não dizer, funcionais, de se sancionar tais condutas socialmente reprováveis.

Cominar penas privativas de liberdade para o acesso não autorizado a sistemas computacionais seria desprezar completamente um potencial intelectual que certamente poderá ser muito bem aproveitado, mormente em um país como o nosso, carente de alta tecnologia e, pior, de professores.

Muitos piratas invadem sistemas como forma de demostrar suas aptidões intelectuais para potenciais empregadores. Encarcerá-los certamente não seria a melhor solução.

Como puní-los então? Obrigando-os a usar seus conhecimentos em prol da sociedade e não contra ela: desenvolvendo programas para instituições públicas, ministrando aulas de informática para a comunidade em geral.

Seria esta uma punição eficaz? Seria quiçá uma pena? Se depender de seu caráter retributivo, vulgo vingança social, provavelmente não. Seus efeitos de prevenção geral, por outro lado, não parecem ser muito superiores àqueles próprios de sentenças cíveis de reparação por danos materiais ou morais. Em termos de prevenção especial, no entanto, parece que há boas chances de a pena alcançar seus objetivos de prevenir a reincidência e ainda de readaptar o condenado ao convívio social.

A solução das penas restritivas de direito é um axioma da constatação da

ineficácia das penas corporais. Optamos simplesmente pelo que aparenta ser uma evolução dos metódos sancionatórios, consagrando as penas de prestação de serviços comunitários como penas principais.

A Teoria da Pena necessita, no entanto, mais do que de uma simples evolução, de uma verdadeira revolução em seus fundamentos, o que decerto não foi nosso objetivo aqui.

Cogitamos até mesmo de silenciar a respeito das penas, mas preferimos fugir ao silêncio obsequioso da omissão, registrando aqui nossa proposta: penas restritivas de direitos para o crime de acesso não autorizado a computadores. Não como alternativas, mas como principais.

Se descumpridas, solução outra não nos resta por ora, senão o retorno ao cárcere medieval.

Melhor não seria o inconstitucional banimento bíblico?

BIBLIOGRAFIA

ADAMSKI, Andrzej. Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. *European colloquiumn on crime and criminal policy*, 6, 1998, Helsinki, Five Issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime Prevention, and Computer Crime. Disponível em: <http://www.vn.fi/om/suomi/heuni/news/fiveissu.pdf>. p. 214-262. Acesso em: 28 de dezembro de 2000.

AHON, Erick Iriarte (Director). *R.E.D.I.*: revista electrónica de Derecho Informático. Disponível em: <http://vlex.com/redi/>. Acesso em: 10 de junho de 2001.

ALEMANHA. *German penal code*. Disponível em: <http://www.bmj.de/publik/e_stgb.pdf >. Acesso em: 3 de junho de 2001.

_____. *Strafgesetzbuch (StGB)*. Disponível em: <http://www.datenschutz-berlin.de/recht/de/rv/szprecht/stgb/index.htm>. Acesso em: 3 de junho de 2001.

ALMEIDA, Carlos Sánchez. *Todo está en venta:* globalizacion, Internet y Derechos Humanos. 2000. 53p. Disponível em: <http://www.kriptopolis.com/docs/enventa.pdf>. Acesso em: 8 de maio de 2001.

ALVES, Maria Bernardete Martins, ARRUDA, Susana Margareth. *Como fazer referências:* bibilográficas, eletrônicas e demais formas de documentos. Disponível em: <http://www.bu.ufsc.br/home982.html>. Acesso em: 8 de maio de 2001.

ANGEL-ANGEL, José de Jesús. *Criptografía Para Principiantes*. 53p. Disponível em: <http://www.kriptopolis.com/docs/criptofund.zip>. Acesso em: 7 de maio de 2001.

AUSTRALIA. *Crimes Act 1914*: act nº 12 as amended. v.1. Disponível em: <http://scaleplus.law.gov.au/html/pasteact/0/28/pdf/Crimes14Vol01.pdf>. Acesso em: 10 de junho de 2001.

_____. *Crimes Act 1914*: act nº 12 as amended. v.2. Disponível em: <http://scaleplus.law.gov.au/html/pasteact/0/28/pdf/Crimes14Vol02.pdf >. Acesso em: 10 de junho de 2001.

BALL, Hill. *Usando Linux*. Rio de Janeiro: Campus, 1999. 650p.

BATISTA, Nilo. *Introdução crítica ao Direito Penal brasileiro*. 4ª ed. Rio de Janeiro: Revan, 2001. 136 p.

BARATTA, Alessandro. *Criminologia crítica e crítica do Direito Penal*: introdução à sociologia do direito penal. 2ª ed. Rio de Janeiro: Freitas Bastos, 1999. 254 p.

BECCARIA, Cesare. *Dos delitos e das penas.* 2ª ed. rev. São Paulo: Editora Revista dos Tribunais, 1999. 149 p.

BÉLGICA. Loi du 28 novembre 2000. Relative à la criminalité informatique. Disponível em: <http://www.droit-technologie.org/fr/legislations/loi_criminalite_informatique_281100.pdf>. Acesso em 10 de junho de 2001.

BRENNER, Susan. Cybercrimes. Designed by Brett Burney. University of Dayton School of Law. Disponível em: <http://cybercrimes.net>. Acesso em: 10 de junho de 2001.

BRENNER, Susan; COCHRAN, Rebecca. *Model State Computer Crimes Code.* Disponível em: <http://www.cybercrimes.net/98MSCCC/files/MSCCC-WordPerfect6-7-8.wpd>. Acesso em: 29 de outubro de 2000.

CANADÁ. *Code ciminel.* Disponível em: <ftp://insight.mcmaster.ca/pub/efc/ccf.txt >. Acesso em: 3 de junho de 2001.

_____. *Criminal Code.* Disponível em: <ftp://insight.mcmaster.ca/pub/efc/cce.txt>. Acesso em: 3 de junho de 2001.

_____. *Criminal Code.* Disponível em: <http://laws.justice.gc.ca/en/C-46/text.html>. Acesso em: 1º de julho de 2001.

CAPEZ, Fernando. *Curso de processo penal.* 5ª ed. rev. São Paulo: Saraiva, 2000. 650 p.

CASACUBERTA, David, MARTÍN MÁS, José Luis. *Diccionario de ciberderechos.* Disponível em: <http://www.kriptopolis.com/dicc.html>. Acesso em 7 de maio de 2001.

CENTER FOR DEMOCRACY AND TECHNOLOGY. *Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25).* Disponível em: <http://www.cdt.org/international/cybercrime/010206cdt.shtml>. Acesso em: 20 de maio de 2001.

COMMELIN, P. *Mitologia grega e romana.* Rio de Janeiro: Ediouro, s/d. 282 p.

CONCERINO, Arthur José. Internet e segurança são compatíveis? In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (coord.). *Direito e Internet:* aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. p. 131-154.

COSTA, Marco Aurélio Rodrigues da. *Crimes de informática.* Disponível em:

<http://www.jus.com.br/doutrina/crinfo.html>. Acesso em: 5 de maio de 2001.

CHAUI, Marilena. *Convite à filosofia*. 12ª ed. São Paulo: Ática, 2000. 440 p.

CHILE. Ley num. 19.223. 7 de Junio de 1993. Ley relativa a delitos informaticos. Disponível em: <http://chile.derecho.org/concepcion/~/legislacion/19223/>. Acesso em: 3 de junho de 2001.

CHINA. *Criminal Law of the People's Republic of China*. Disponível em: <http://www.qis.net/chinalaw/prclaw60.htm>. Acesso em: 10 de junho de 2001.

COMISSÃO DAS COMUNIDADES EUROPÉIAS. *Comunicação da comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões*: criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade. Bruxelas, 2000. 39p. Disponível em: <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComPT.pdf>. Acesso em: 20 de maio de 2001.

COUNCIL OF EUROPE. European Committee on Crime Problems. Committee of Experts on Crime in Cyber-Space. *Explanatory Memorandum Related Thereto*. Strasbourg, 29 June 2001. Disponível em: <http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm>. Acesso em: 29 de junho de 2001.

_____. *Draft Convention on Cyber-crime (Final Activity Report)*. Strasbourg, 29 June 2001. Disponível em: <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>. Acesso em: 29 de junho de 2001.

_____. *Draft Convention on Cyber-crime (Draft N° 27 REV.) and Explanatory Memorandum Related Thereto*. Strasbourg, 25 May 2001. Disponível em: <http://conventions.coe.int/treaty/EN/projets/cybercrime27.doc>. Acesso em: 10 de junho de 2001.

_____. *Draft Convention on Cyber-crime (Draft N° 25 REV.)*. Strasbourg, 27 December 2000. Disponível em: <http://www.cdt.org/international/cybercrime/001225cybercrime25.pdf>. Acesso em: 28 de dezembro de 2000.

CULT_HERO et al. *Attrition*. Disponível em: <http://www.attrition.org>. Acesso em: 10 de junho de 2001.

DAOUN, Alexandre Jean, BLUM, Renato M. S. Opice. Cybercrimes. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (coord.). *Direito e Internet: aspectos jurídicos relevantes*. Bauru: EDIPRO, 2000. p. 117-129.

DELMANTO, Celso, DELMANTO, Roberto, DELMANTO JÚNIOR, Roberto. *Código penal comentado*. 4.ed. Rio de Janeiro: Renovar, 1998. 961 p.

DENNING, Dorothy E. *Cyberterrorism.* Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>. Acesso em: 7 de maio de 2001.

_____. *Reflections on cyberweapons controls.* Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc >. Acesso em: 7 de maio de 2001.

_____. *Concerning Hackers Who Break into Computer Systems.* Disponível em: <http://www.cpsr.org/ftp/cpsr/computer_crime/denning_defense_hackers.txt>. Acesso em: 4 de janeiro de 2001.

_____. *Activism, Hacktivism, and Cyberterrorism*: The Internet as a Tool for Influencing Foreign Policy. Disponível em: <http://www.nautilus.org/info-policy/workshop/papers/denning.html>. Acesso em: 7 de maio de 2001.

DENNING, Dorothy E.; BAUGH JR., William E. *Hiding Crimes in Cyberspace.* Disponível em: <http://www.cs.georgetown.edu/%7Edenning/crypto/hiding1.doc>. Acesso em: 28 de dezembro de 2000.

DUTHIL, Daniel (Directeur de publication). *Code Silex de l'informatique.* Disponível em: <http://www.celog.fr/silex/tome1/sommaire.htm>. Acesso em: 10 de junho de 2001.

ESPANHA. Ley Orgánica 15 de 13 de diciembre de 1999. Protección de datos de carácter personal. Disponível em: <http://www.ctv.es/USERS/chiri/htm/lopd.htm>. Acesso em: 3 de junho de 2001.

ESTADOS UNIDOS DA AMÉRICA. United States Code. Title 18 – Crimes and criminal procedure. Disponível em: <http://uscode.house.gov/DOWNLOAD/Title_18.ZIP>. Acesso em: 10 de junho de 2001.

_____. United States Code. Title 18 – Crimes and criminal procedure. Chapter 47 – Fraud and false statements. Sec. 1030. Fraud and related activity in connection with computers. Disponível em: <http://www4.law.cornell.edu/uscode/unframed/18/1030.html>. Acesso em: 10 de junho de 2001.

_____. *Computer Crime Statutes.* Disponível em: <http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Legal/comp_crime_us_state.laws>. Acesso em: 15 de junho de 2000.

FERREIRA, Aurélio Buarque de Holanda. *Dicionário Aurélio eletrônico*: século XXI. v.3.0. Rio de Janeiro: Nova Fronteira, nov. 1999. CD-ROM.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton

de, SIMÃO FILHO, Adalberto (coord.). *Direito e Internet*: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. p. 207-237.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Petrópolis: Vozes, 1987. 262p.

FRAGOSO, Heleno Cláudio. *Lições de direito penal*: a nova parte geral. 8ª ed. Rio de Janeiro: Forense, 1985. 491 p.

_____. *Lições de direito penal*: parte especial: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983. 615 p.

FRANÇA, Júnia Lessa. *Manual para normalização de publicações técnico-científicas*. 4 ed. rev. e aum. Belo Horizonte: Ed. UFMG, 1998. 213p.

FRANÇA. *Code de procédure pénale*. Disponível em: <http://fabrice.gauthier.free.fr/fabrice/fichiers/pdf/cpppdf.zip>. Acesso em: 11 de janeiro de 2001.

_____. *Code pénal*. Disponível em: <http://fabrice.gauthier.free.fr/fabrice/fichiers/pdf/cppdf.zip>. Acesso em: 11 de janeiro de 2001.

FRANCO, Alberto Silva *et al*. *Código penal e sua interpretação jurisprudencial*. 2ª ed. rev. ampl. São Paulo: Editora Revista dos Tribunais, 1987. 1479 p.

FRANKLIN, Darren. *Hanging a shingle on the information superhighway*: legal advice on the internet and the problems of prohibited client solicitation and unintended attorney-client relationships. Stanford Technology Law Review. 8 p. Disponível em: <http://stlr.stanford.edu/STLR/Articles/01_STLR_2/article_pdf.pdf>. Acesso em: 8 de maio de 2001.

FUOCO, Taís. Maconha é oferecida em leilões da Ebay. *Plantão Info*. Disponível em: <http://www2.uol.com.br/info/infonews/091999/24091999-2.shl>. Acesso em: 25 de setembro de 1999.

GARCÍA-PABLOS DE MOLINA, Antonio; GOMES, Luiz Flávio. *Criminologia*: introdução a seus fundamentos teóricos: introdução às bases criminológicas da Lei 9.099/95, lei dos juizados criminais. 3 ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2000. 536 p.

GEHRINGER, Max, LONDON, Jack. Odisséia Digital. *Vip Exame*, São Paulo: Abril, a. 20, n. 4, abr. 2001. Suplemento especial.

GÓMEZ, José Manuel (Director). *Kriptópolis*. Disponível em: <http://www.kriptopolis.com>. Acesso em: 10 de junho de 2001.

GONÇALVES, Marcus. *Firewalls*: guia completo. Rio de Janeiro: Ciência Moderna, 2000. 632p.

GOUVÊA, Sandra. *O direito na era digital*: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. 163p.

GREGO, Maurício. Hackers. *Info Exame*, São Paulo: Abril, a. 16, n. 179, p. 32-40, fev. 2001.

_____. O submundo dos hackers. *Info Exame*, São Paulo: Abril, a. 15, n. 173, p. 46-58, ago. 2000.

HERNÁNDEZ, Claudio. *Hackers*: los clanes de la red. 107p. Disponível em: <http://www.kriptopolis.com/docs/hackers.zip>. Acesso em: 7 de maio de 2001.

HOWARD, John D. *An analysis of security incidents on the Internet*: 1989-1995. Pittsburgh: Carnegie Mellon University, 1997. Disponível em: <http://www.cert.org/research/JHThesis/Start.html>. Acesso em: 5 de janeiro de 2001. (Dissertation, Doctor of Philosophy)

HUNGRIA, Nélson. *Comentários ao Código Penal*: vol. I, tomo II: art. 11 a 27. 4ª ed. Rio de Janeiro: Forense, 1958. 549 p.

ITÁLIA. *Codice penale*. Disponível em: <http://www.studiocelentano.it/cp/codicepenale000.htm>. Acesso em: 11 de janeiro de 2001.

JAEGER, Werner Wilhelm. *Paidéia*: a formação do homem grego. 3ª ed. São Paulo: Martins Fontes, 1994. 1.413 p.

JAKOBS, Günther. *A imputação objetiva no Direito Penal*. São Paulo: Revista dos Tribunais, 2000. 94 p.

LARANJA Mecânica. Direção, Produção e Roteiro: Stanley Kubrick. Intérpretes: Patrick Magee; Adrienne Corri; Mirian Karlan; Malcolm McDowell e outros. Warner Home Video, 1971. 1 fita de vídeo (138 min), VHS, son., color. Baseado no livro de Anthony Burgess.

LISBOA, Roberto Senise. A inviolabilidade de correspondência na Internet. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (coord.). *Direito e Internet*: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. p. 465-491.

LITTMAN, Jonathan. *O jogo do fugitivo*: em linha direta com Kevin Mitnick. Rio de Janeiro: Rocco, 1996. 399p.

_____. *Watchman*: a vida excêntrica e os crimes do serial hacker Kevin Poulsen. Rio de Janeiro: Record, 1998. 363 p.

LOPES, Jair Leonardo. *Curso de Direito Penal*: parte geral. 3.ed. rev. e atual. São Paulo, Revista dos Tribunais, 1999. 281 p.

LÓPEZ, Manuel José Lucena. *Criptografía y seguridad en computadores*. 2ª ed. Departamento de Informática Escuela Politécnica Superior Universidad de

Jaen, septiembre de 1999. 167p. Disponível em: <ftp://www.etsimo.uniovi.es/pub/network/security/criptografia.zip>. Acesso em: 8 de maio de 2001.

MACHADO, Cynthia Semíramis Figueiredo. Da proteção penal a direitos autorais sobre softwares. *Boletim do Instituto de Ciências Penais,* Belo Horizonte, a. 2, n. 16, p. 6-8, jun. 2001.

MAGALHÃES, José Luiz Quadros de. *Direito Constitucional.* Belo Horizonte: Mandamentos, 2000.

MARQUES, Daniela de Freitas. *Elementos subjetivos do injusto.* Belo Horizonte: Del Rey, 2001. 160p.

MARTORELL, Manuel Pons. *Control de accesos.* 42p. Disponível em: <http://www.kriptopolis.com/docs/accesos.zip>. Acesso em: 7 de maio de 2001.

MATTOS, Virgílio. *Trem de doido*: o direito penal e a psiquiatria de mãos dadas. Belo Horizonte: Una Editoria, 1999. 175 p.

MAXIMILIANO, Carlos. *Hermenêutica e aplicação do direito.* 16ª ed. Rio de Janeiro: Forense, 1997. 426p.

MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hackers expostos*: segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2000. 469 p.

MELO, Aline Mary Moreira de. *Os crimes de informática e suas formas de punições em relação ao direito.* Disponível em: <http://www.cbeji.com.br/artigos/artalinemary04062001.htm>. Acesso em: 18 de junho de 2001.

MENTOR, The. *The conscience of a hacker.* Disponível em: <http://www.attrition.org/~modify/texts/ethics/hackers_manifesto.html>. Acesso em: 5 de janeiro de 2001.

MÉXICO. *Codigo Penal Federal.* Disponível em: <http://www.cddhcu.gob.mx/leyinfo/pdf/11.pdf>. Acesso em: 10 de junho de 2001.

MIRABETE, Julio Fabbrini. *Código penal interpretado.* São Paulo: Atlas, 1999. 1.972 p.

_____. *Código de processo penal interpretado*: referências doutrinárias, indicações legais, resenha jurisprudencial. 6ª ed. São Paulo: Atlas, 1999. 957 p.

NEMEROFSKY, Jeff . *The crime of "interruption of computer services to authorized users":* Have you ever heard of it? Disponível em:

<http://www.richmond.edu/jolt/v6i5/article2.html>. Acesso em: 29 de outubro de 2000.

NEW JERSEY. Commission of Investigation. Computer Crime - A Joint Report. Disponível em: <http://www.state.nj.us/sci/computer.pdf>. Acesso em: 5 de janeiro de 2001.

PAULINO, Wilson Roberto. *Biologia atual*: seres vivos, fisiologia, embriologia. 4 ed. São Paulo: Ática, 1990. v. 2, 328 p.

PAVARINI, Massimo. *Los confines de la cárcel*. Montevideo: Carlos Alvarez Editor, 1995.

PIAUHYLINO, Luiz [Luiz Piauhylino de Mello Monteiro]. Projeto de Lei nº 84 de 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/LuizPiauhylino/textopl84.doc>. Acesso em: 11 de junho de 2001.

PIMENTEL, Alexandre Freire. *O direito cibernético*: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000. 267 p.

PIRES, Ariosvaldo de Campos. *Compêndio de Direito Penal:* parte especial: crimes contra a pessoa; crimes contra o patrimônio: artigos 121 a 183. Rio de Janeiro: Forense, *1990. 291* p.

_____. *A coação irresistível no Direito Penal brasileiro*. 2ª ed. Belo Horizonte: Lemi, 1973. 72 p.

POPPER, Karl. *Ciência, conjecturas e refutações*. Brasília: UNB, 1982.

PORTUGAL. Lei nº 109, de 17 de agosto de 1991. Criminalidade Informática. Disponível em: <http://www.terravista.pt/mussulo/1139/crimi.html>. Acesso em: 10 de junho de 2001.

PRADO, Luís Régis. *Curso de Direito Penal Brasileiro*: parte geral. 2.ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2000. 632 p.

RAMOS, Beatriz Vargas. *Do concurso de pessoas*: contribuição ao estudo do tema na nova parte geral do código penal. Belo Horizonte: Del Rey, 1996. 208 p.

REINO UNIDO. Computer Misuse Act 1990 (c.18). 29th June 1990. An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes. Disponível em: <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm>. Acesso em 10 de junho de 2001.

REIS, Maria Helena Junqueira. *Computer crimes*: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1996. 62 p.

REZENDE, Pedro Antonio Dourado de. *Internet, riscos e falácias*: os protocolos de autenticação. Disponível em: <http://www.observatoriodaimprensa.com.br/artigos/eno050920001.htm>. Acesso em: 10 de junho de 2001.

_____. *Palavras mágicas*: sobre entidades certificadoras, assinaturas eletrônicas e projetos de lei. Disponível em: <http://www.cic.unb.br/docentes/pedro/trabs/oab.htm>. Acesso em: 10 de junho de 2001.

ROBINSON, James K. *Internet as the scene of crime*. Disponível em: <http://www.usdoj.gov/criminal/cybercrime/roboslo.htm>. Acesso em: 8 de janeiro de 2001.

ROCHA, Fernando Antônio Nogueira Galvão da. *Criminalidade do computador*. Revista Jurídica do Ministério Público, Belo Horizonte, a. 27, v. 19, p. 75-98, 1996.

ROGERS, Marc. *The future of information security assurance*. Disponível em: <http://www.escape.ca/~mkr/isaca.ppt>. Acesso em: 28 de dezembro de 2000.

_____. *A new hacker taxonomy*. Disponível em: <http://www.escape.ca/~mkr/hacker_doc.pdf>. Acesso em: 28 de dezembro de 2000.

_____. *Information warfare, cyber-terrorism, cyber-criminals*. Disponível em: <http://www.escape.ca/~mkr/cyberterror.ppt>. Acesso em: 28 de dezembro de 2000.

_____. *Modern-day Robin Hood or moral disengagement*: understanding the justification for criminal computer activity. Disponível em: <http://www.escape.ca/~mkr/moral_doc.pdf>. Acesso em: 28 de dezembro de 2000.

_____. *Organized computer crime and more sophisticated security controls*: Which Came First the Chicken or the Egg? Disponível em: <http://www.escape.ca/~mkr/Org_doc.pdf>. Acesso em: 28 de dezembro de 2000.

_____. *Psychological theories of crime and hacking*. Disponível em: <http://www.escape.ca/~mkr/crime_doc.pdf>. Acesso em: 28 de dezembro de 2000.

_____. *Security threats*. Disponível em: <http://www.escape.ca/~mkr/apegm.ppt>. Acesso em: 28 de dezembro de 2000.

_____. *The need for a balanced security posture*. Disponível em: <http://www.escape.ca/~mkr/balanced_doc.pdf>. Acesso em: 28 de dezembro de 2000.

ROHRMANN, Carlos Alberto. *O Direito Virtual:* a assinatura digital e os contratos comerciais eletrônicos. Belo Horizonte, 1999. 134f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Minas Gerais.

ROTEMBERG, Marc. *Fair information practices and the architecture of privacy*: what larry doesn't get. Stanford Technology Law Review. 34 p. Disponível em: <http://stlr.stanford.edu/STLR/Articles/01_STLR_1/article_pdf.pdf>. Acesso em: 8 de maio de 2001.

ROXIN, Claus. *Política Criminal e sistema jurídico-penal.* Rio de Janeiro: Renovar, 2000. 99 p.

SACCONI, Luiz Antonio. *Nossa Gramática*: teoria. 11 ed. reform. e rev. São Paulo: Atual, 1990. 465 p.

SALES, Sheila Jorge Selim de. *Do sujeito ativo:* na parte especial do Código Penal. Belo Horizonte: Del Rey, 1993. 159 p.

SCHJOLBERG, Stein. *The legal framework*. Disponível em: <http://www.mossbyrett.of.no/info/legal.html>. Acesso: em 10 de junho de 2001.

SCORPIO. *My code of ethics.* Disponível em: <http://www.attrition.org/~modify/texts/ethics/my.code.of.ethics.html>. Acesso: em 5 de janeiro de 2001.

SEGURANÇA Máxima: o guia de um hacker para proteger seu site na internet e sua rede. 2.ed. Rio de Janeiro: Campus, 2000. 826 p. (anônimo).

SHAW, Eric; RUBY, Keven G.; POST, Jerrold M. The insider threat to information systems - *The psychology of the dangerous insider*. Disponível em: <http://www.escape.ca/~mkr/sab.pdf>. Acesso em: 28 de dezembro de 2000.

SIEBER, U. *Computer crime and criminal information law*: new trends in the international risk and information society. Disponível em: <http://www.jura.uni-wuerzburg.de/sieber/mitis/ComCriCriInf.htm>. Acesso em: 29 de outubro de 2000.

SILVA NETO, Amaro Moraes e. *Resgatemos os hackers.* Disponível em: <http://www.jus.com.br/doutrina/hackers.html>. Acesso em: 5 de maio de 2001.

SINROD, Eric J., JOLISH, Barak D. *Controlling chaos*: the emerging law of privacy and speech in cyberspace. Stanford Technology Law Review. 18 p. Disponível em: <http://stlr.stanford.edu/STLR/Articles/99_STLR_1/article_pdf.pdf>. Acesso em: 8 de maio de 2001.

STERLING, Bruce. *The hacker crackdown (la caza de hackers):* ley y desorden en la frontera eletrónica. 214p. Disponível em: <http://www.kriptopolis.com/docs/hackercdown.zip>. Acesso em: 7 de maio de

2001.

_____. _____. 279p. Disponível em: <http://www.globaldrome.org/textos/hackercrack/pdf.zip>. Acesso em: 7 de maio de 2001.

SUÉCIA. *The penal code*. Disponível em: <http://wings.buffalo.edu/law/bclc/sweden.pdf>. Acesso em: 1º de julho de 2001.

SUIÇA. *Códe penal suisse*. Disponível em: <http://www.admin.ch/ch/f/rs/3/311.0.fr.pdf>. Acesso em: 10 de junho de 2001.

TAVARES, Juarez. *Teoria do injusto penal*. Belo Horizonte: Del Rey, 2000. 335 p.

TOLEDO, Francisco de Assis. *Princípios Básicos de Direito Penal*. 5ª ed. São Paulo: Saraiva, 1994. 362 p.

TORRES, Gabriel. *Hardware*: Curso Completo. 3 ed. Rio de Janeiro: Axcel Books, 1999. 1.147 p.

TORVALDS, Linus, DIAMOND, David. *Só por prazer*: Linux, os bastidores da criação. Rio de Janeiro: Campus, 2001. 297 p.

TOSI, Renzo. *Dicionário de sentenças latinas e gregas*. São Paulo: Martins Fontes, 1996. 904 p.

UNITED STATES DEPARTMENT OF JUSTICE. The Computer Crime and Intellectual Property Section. The National Information Infrastructure Protection Act of 1996: legislative analysis. Disponível em: <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>. Acesso em: 10 de junho de 2001.

VALLIM, Celso Henrique de Castro Baptista. *Crimes contra a honra na Internet*. Florianópolis: Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina, 2000. 52 p. Disponível em: <http://buscalegis.ccj.ufsc.br/arquivos/ccj/mono-crimescahni.pdf>. Acesso em: 13 de abril de 2001. (Monografia, Graduação em Direito).

VARELLA, Drauzio. *Estação Carandiru*. São Paulo: Companhia das Letras, 1999. 297 p.

VELLOSO, Fernando de Castro. *Informática*: conceitos básicos. 4ª ed. rev. e atual. Rio de Janeiro: Campus, 1999.

VIANNA, Túlio Lima. Dos Crimes pela Internet. *Revista do CAAP*, Belo Horizonte, 2001. (No prelo).

_____. Cibernética Penal. *Boletim do Instituto de Ciências Penais*, Belo

Horizonte, a. 2, n. 16, p. 4-6, jun. 2001.

_____. Dos Crimes por Computador. *Revista do CAAP*, Belo Horizonte, a. 4, n. 6, p. 463-491, 1999.

_____. Prolegômenos à hermenêutica jurídica. *Revista do CAAP*, Belo Horizonte, a. 3, n. 4, p. 243-263, 1998.

WALKER, David B. *Privacy in the Digital Age*: encryption policy–a call for congressional action. Stanford Technology Law Review. 60 p. Disponível em: <http://stlr.stanford.edu/STLR/Articles/99_STLR_3/article_pdf.pdf>. Acesso em: 8 de maio de 2001.

WALKER, Kent. *Where everybody knows your name*: a pragmatic look at the costs of privacy and the benefits of information exchange. Stanford Technology Law Review. 50p. Disponível em: <http://stlr.stanford.edu/STLR/Articles/00_STLR_2/article_pdf.pdf>. Acesso em: 8 de maio de 2001.

WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET. The Electronic Frontier: the challenge of unlawful conduct involving the use of the internet. Disponível em: <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>. Acesso em: 8 de janeiro de 2001.

ZAFFARONI, Eugenio Raúl, PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro*: parte geral. 2.ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 1999. 888 p.

ZEVIAR-GEESE, Gabriole. *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet*. Disponível em: <http://law.gonzaga.edu/borders/documents/cyberlaw.htm>. Acesso em: 29 de outubro de 2000.

ANEXO A

Legislação Estrangeira

ALEMANHA:

http://www.datenschutz-berlin.de/recht/de/rv/szprecht/stgb/index.htm

STRAFGESETZBUCH (StGB)

§ 202a Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, ma- gnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er

1. eine Tat nach § 303a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303c Strafantrag

In den Fällen der §§ 303 bis 303b wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Tradução não oficial para a língua inglesa:

http://www.bmj.de/publik/e_stgb.pdf

German Penal Code

Section 202a Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with.imprisonment for not more than three years or a fine.
(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

Section 303a Alteration of Data
(1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (Section 202a subsection (2)), shall be punished with imprisonment for not more than two years or a fine.
(2) An attempt shall be punishable..

Section 303b Computer Sabotage
(1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another or a public authority by:
1. committing an act under Section303a subsection (1); or
2. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be punished with imprisonment for not more than five years or a fine.
(2) An attempt shall be punishable.

Section 303c Application for Criminal Prosecution
In cases under Sections 303 to 303b the act shall only be prosecuted upon complaint, unless the prosecuting authority considers ex officio that it is required to enter the case because of the special public interest therein.

AUSTRÁLIA

http://scaleplus.law.gov.au/html/pasteact/0/28/pdf/Crimes14Vol01.pdf

Crimes Act 1914 (Act No. 12 of 1914 as amended)

Part VIA—Offences relating to computers

76A Interpretation

(1) In this Part, unless the contrary intention appears:

carrier means:

(a) a carrier (within the meaning of the Telecommunications Act 1997); or

(b) a carriage service provider (within the meaning of that Act).

Commonwealth includes a public authority under the Commonwealth.

Commonwealth computer means a computer, a computer system or a part of a computer system, owned, leased or operated by the Commonwealth.

data includes information, a computer program or part of a computer program.

(2) In this Part:

(a) a reference to data stored in a computer includes a reference to data entered or copied into the computer; and

(b) a reference to data stored on behalf of the Commonwealth in a computer includes a reference to:

(i) data stored in the computer at the direction or request of the Commonwealth; and

(ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.

76B Unlawful access to data in Commonwealth and other computers

(1) A person who intentionally and without authority obtains access to:

(a) data stored in a Commonwealth computer; or

(b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence.

Penalty: Imprisonment for 6 months.

(2) A person who:

(a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(3) A person who:

(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(4) For the purposes of an offence against subsection (1), (2) or (3), absolute liability applies to whichever one of the following physical elements of circumstance is relevant to the offence:

(a) that the computer is a Commonwealth computer;

(b) that the computer is not a Commonwealth computer.

Note: For absolute liability, see section 6.2 of the Criminal Code.

76C Damaging data in Commonwealth and other computers

(1) A person who intentionally and without authority:

(a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;

(c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence.

Penalty: Imprisonment for 10 years.

(2) For the purposes of an offence against subsection (1), absolute liability applies to whichever one of the following physical elements of circumstance is relevant to the offence:

(a) that the computer is a Commonwealth computer;

(b) that the computer is not a Commonwealth computer.

Note: For absolute liability, see section 6.2 of the Criminal Code.

76D Unlawful access to data in Commonwealth and other computers by means of Commonwealth facility

(1) A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence.

Penalty: Imprisonment for 6 months.

(2) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, with intent to defraud any person and without authority obtains access to data stored in a computer; or

(b) by means of such a facility, intentionally and without authority obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defence or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(3) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, has intentionally and without authority obtained access to data stored in a computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

is guilty of an offence.

Penalty: Imprisonment for 2 years.

(4) For the purposes of an offence against subsection (1), (2) or (3), absolute liability applies to the physical element of circumstance of the offence, that the facility is operated or provided by the Commonwealth or by a carrier.

Note: For absolute liability, see section 6.2 of the Criminal Code.

76E Damaging data in Commonwealth and other computers by means of Commonwealth facility

(1) A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority:

(a) destroys, erases or alters data stored in, or inserts data into, a computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;

is guilty of an offence.

Penalty: Imprisonment for 10 years.

(2) For the purposes of an offence against subsection (1), absolute liability applies to the physical element of circumstance of the offence, that the facility is operated or provided by the Commonwealth or by a carrier.

Note: For absolute liability, see section 6.2 of the Criminal Code.

76F Saving of State and Territory laws

Sections 76D and 76E are not intended to exclude or limit the concurrent operation of any law of a State or Territory.

BÉLGICA

http://www.droit-technologie.org/fr/legislations/loi_criminalite_informatique_281100.pdf

Le Code Penal – Livre II

Titre IXbis. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes.

Art. 550bis.

§1 er . Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprison-nement de trois mois à un an et d'une amende de vingt-six

francs à vingt-cinq mille francs ou d'une de ces peines seulement. Si l'infraction visée à l'alinéa 1 er , est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement.

§ 3. Celui qui se trouve dans une des situations visées aux §§ 1 er et 2 et qui : 1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique; 2° soit fait un usage quelconque d'un système informatique appar-tenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers; 3° soit cause un dommage quelconque, meˆme non intentionnelle-ment, au système informatique ou aux données qui sont stockéestraitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système; est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six francs belges à cinquante mille francs ou d'une de ces peines seulement.

§ 4. La tentative de commettre une des infractions visées aux §§ 1 er et 2 est punie des meˆmes peines.

§ 5. Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1 er à 4 peuvent eˆtre commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1 er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent francs à deux cent mille francs ou d'une de ces peines seulement.

§ 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1 er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.

§ 8. Les peines prévues par les §§ 1 er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550ter.

CANADÁ

http://laws.justice.gc.ca/en/C-46/text.html

Criminal Code
CHAPTER C-46

Unauthorized use of computer

342.1 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Definitions

(2) In this section,

"computer password" « mot de passe »

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" «programme d'ordinateur»

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" «service d'ordinateur»

"computer service" includes data processing and the storage or retrieval of data;

"computer system" «ordinateur»

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" «données" — "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" «dispositif électromagnétique, acoustique, mécanique ou autre» — "electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" «fonction» — "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" «intercepter» — "intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

"traffic" « trafic » — "traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.

Possession of device to obtain computer service — 342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

Forfeiture — (2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered

forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Limitation

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 19.

CHILE

http://chile.derecho.org/concepcion/~/legislacion/19223/

DIARIO OFICIAL DE LA REPUBLICA DE CHILE - 7 de Junio de 1993

Normas Generales
PODER LEGISLATIVO
Ministerio del Justicia
SUBSECRETARIA DE JUSTICIA

LEY NUM. 19.223
LEY RELATIVA A DELITOS INFORMATICOS

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia.

Lo que transcribo a Ud. para su conocimiento.-

Saluda atentamente a Ud., Martita Worner Tapia, Subsecretario de Justicia.

CHINA

http://www.qis.net/chinalaw/prclaw60.htm

Criminal Law of the People's Republic of China

(Adopted by the Second Session of the Fifth National People's Congress on July 1, 1979 and amended by the Fifth Session of the Eighth National People's Congress on March 14, 1997)

Article 284. Whoever illegally uses special monitoring or photographing equipment and causes grave consequences is to be sentenced to not more than two years of fixed-term imprisonment, criminal detention, or control.

Article 285. Whoever violates state regulations and intrudes into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.

Article 286. Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.

Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.

Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.

Article 287. Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

ESTADOS UNIDOS

http://www4.law.cornell.edu/uscode/unframed/18/1030.html

- United States Code
  - TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
    - PART I - CRIMES
      - CHAPTER 47 - FRAUD AND FALSE STATEMENTS
      -

Sec. 1030. Fraud and related activity in connection with computers

- (a) Whoever -
  - (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
  - (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -
    - (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are

defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

- (B) information from any department or agency of the United States; or
- (C) information from any protected computer if the conduct involved an interstate or foreign communication;

- (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
- (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
- (5)
  - (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
  - (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
  - (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;
- (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -
  - (A) such trafficking affects interstate or foreign commerce; or
  - (B) such computer is used by or for the Government of the United States; [1]
- (7) with intent to extort from any person, firm, association, educational institution, financial institution, government

entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

- (b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
- (c) The punishment for an offense under subsection (a) or (b) of this section is -
- (1)
    - (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (2)
    - (A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [2]
    - (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if -
        - (i) the offense was committed for purposes of commercial advantage or private financial gain;
        - (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
        - (iii) the value of the information obtained exceeds $5,000; [3]
    - (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt

to commit an offense punishable under this subparagraph; and (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [4]

- (d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B),
  - () The United States Secret Service shall, in addition to any of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
  - (e) As used in this section -
    - (1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
    - (2) the term "protected computer" means a computer -
      - (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
      - (B) which is used in interstate or foreign commerce or communication;

- (3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
- (4) the term "financial institution" means -
  - (A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
  - (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
  - (C) a credit union with accounts insured by the National Credit Union Administration;
  - (D) a member of the Federal home loan bank system and any home loan bank;
  - (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
  - (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
  - (G) the Securities Investor Protection Corporation;
  - (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
    (I) an organization operating under section 25 or section 25(a) [5] of the Federal Reserve Act. [6]
- (5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
- (6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
- (7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and [7]
- (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that -
  - (A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

- (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;
- (C) causes physical injury to any person; or
- (D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

- (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
- (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.
- (h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

Footnotes

[1] So in original. Probably should be followed by "or".

[2] So in original. The word "and" probably should not appear.

[3] So in original. Probably should be followed by "and".

[4] So in original. The "; and" probably should be a period.

[5] See References in Text note below.

[6] So in original. The period probably should be a semicolon.

[7] So in original. The word "and" probably should not appear.

FRANÇA

http://fabrice.gauthier.free.fr/fabrice/fichiers/pdf/cppdf.zip

Le Code Penal

Les atteintes aux systèmes de traitement automatisé de données.

Article 323-1.
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 F d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende.

Article 323-2.
Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

Article 323-3.
Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende.

Article 323-4.
La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5.
Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l' article 131-26 ;
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée a commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; 225 Atteintes aux systèmes informatiques.5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

.

Article 323-6.
Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 , des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :
1° L'amende, suivant les modalités prévues par l'article 131-38 ;
2° Les peines mentionnées à l'article 131-39 .
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7.
La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines.

ITÁLIA

http://www.studiocelentano.it/cp/codicepenale002a.htm

Codice Penale

Art. 615 ter
- Accesso abusivo ad un sistema informatico o telematico -
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita

anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o *alla sicurezza pubblica o alla sanità o alla* protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio (1).

(1)Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

Art. 615 quater

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici -

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni.

La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater (1).

(1) Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

Art. 615 quinquies

- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico -

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni (1).

(1)Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

MÉXICO

http://www.cddhcu.gob.mx/leyinfo/pdf/11.pdf

Codigo Penal Federal (Ultima reforma aplicada 12/06/2000)

LIBRO SEGUNDO

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

Capitulo II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis1

Al que sin autorizacion modifique, destruya o provoque *pérdida de información* contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida em sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prision y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán e uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financeiro, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financeiro, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financeiro, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financeiro, indebidamente copie información que contengan, se le impondrán de tres meses a dos anõs de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financeiro.

Artículo 211 bis 6

Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financeiro, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7

Las penas previstas en este capítulo se aumentarán hasta en una mítad cuando la información obtenida se utilice en provecho proprio o ajeno.

PORTUGAL

http://www.terravista.pt/mussulo/1139/crimi.html

Lei da Criminalidade Informática
Criminalidade Informática-Lei n.º109/91, 17 de Agosto

A Assembleia da República decreta nos termos dos artigos 164.º, alínea d), 168.º, n.º1, alínea c), e 169.º, n.º3, da Constituição, o seguinte:

CAPÍTULO I - Princípios gerais

Art. 1º Legislação penal

Aos crimes previstos na presente lei são subsidiariamente aplicáveis as disposições do Código Penal.

Art. 2º Definições

Para efeitos da presente lei, considera-se:

a) Rede informática - um conjunto de dois ou mais computadores interconectados;

b) Sistema informático - um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados;

c) Programa informático - um conjunto de instruções capazes, quando inseridos num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado;

d) Topografia - uma série de imagens entre si ligadas, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

e) Produto semicondutor - a forma final ou intermédio de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não,

uma função electrónica;

f) Intercepção - o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

g) Valor elevado - aquele que exceder 50 unidades de conta processual penal avaliadas no momento da prática do facto;

h) Valor consideravelmente elevado aquele que exceder 200 unidades de conta processual penal avaliadas no momento da prática do facto.

Art. 3º Responsabilidade penal das pessoas colectivas e equiparadas

1. As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes.

2. A responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.

3. A responsabilidade das entidades referidas no nº 1 não exclui a responsabilidade individual dos respectivos agentes.

4. As entidades referidas no nº 1 respondem solidariamente, nos termos da lei civil, pelo pagamento das multas, indemnizações e outras prestações em que forem condenados os agentes das infracções previstas na presente lei.

CAPÍTULO II - Dos crimes ligados à informática

Art. 4º Falsidade informática

1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

2. Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas

informatizados que foram objecto dos actos referidos no número anterior, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.

3. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de um a cinco anos.

Art. 5º Dano relativo a dados ou programas informáticos

1. Quem, sem para tanto estar autorizado, e actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectar a capacidade de uso será punido corri pena de prisão até três anos ou pena de multa.

2. A tentativa é punível.

3. Se o dano causado for de valor elevado, a pena será a de prisão até 5 anos ou de multa até 600 dias.

4. Se o dano causado for de valor consideravelmente elevado, a pena será a de prisão de 1 a 10 anos.

5. Nos casos previstos nos nºs 1, 2 e 3 o procedimento penal depende da queixa.

Art. 6º Sabotagem informática

1. Quem introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2. A pena será a de prisão de um a cinco anos se o dano emergente da perturbação for de valor elevado.

3. A pena será a de prisão de 1 a 10 anos se o dano emergente da perturbação for de valor consideravelmente elevado.

Art. 7º Acesso ilegítimo

1. Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até um ano ou com pena de multa até 120 dias.

2. A pena será a de prisão até três anos ou multa se o acesso for conseguido através da violação de regras de segurança.

3. A pena será a de prisão de um a cinco anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

4. A tentativa é punível.

5. Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa.

Art. 8º Intercepção ilegítima

1. Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa.

2. A tentativa é punível.

Art. 9º Reprodução ilegítima de programa protegido

1. Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa.

2. Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3. A tentativa é punível.

Art. 10º Penas aplicáveis às pessoas colectivas e equiparadas

1. Pelos crimes previstos na presente lei são aplicáveis às pessoas colectivas e equiparadas as seguintes penas principais:

a) Admoestação;

b) Multa;

c) Dissolução.

2. Aplica-se a pena de admoestação sempre que, nos termos gerais. tal pena possa ser aplicada à pessoa singular que, em representação e no interesse da pessoa colectiva ou equiparada, tiver praticado o facto.

3. Quando aplicar a pena de admoestação, o tribunal poderá aplicar cumulativamente a pena acessória de caução de boa conduta.

4. Cada dia de multa corresponde a uma quantia entre 10 000$ e 200 000$, que o tribunal fixará em função da situação económica e financeira da pessoa colectiva ou equiparada e dos seus encargos.

5. Se a multa for aplicada a uma entidade sem personalidade jurídica, responderá por ela o património comum e, na sua falta ou insuficiência, o património de cada um dos associados.

6. A pena de dissolução só será aplicada quando os titulares dos órgãos ou representantes da pessoa colectiva ou sociedade tenham agido com a intenção, exclusiva ou predominantemente, de, por meio dela, praticar os factos que integram os crimes previstos na presente lei ou quando a prática reiterada desses factos mostre que a pessoa colectiva ou sociedade está a ser utilizada para esse efeito, quer pelos seus membros, quer por quem exerça a respectiva administração.

CAPÍTULO III - Penas acessórias

Art. 11º Penas acessórias

Relativamente aos crimes previstos no presente diploma, podem ser aplicadas as seguintes penas acessórias:

a) Perda de bens;

b) Caução de boa conduta;

c) Interdição temporária do exercício de certas actividades ou profissões;

d) Encerramento temporário do estabelecimento;

e) Encerramento definitivo do estabelecimento;

f) Publicidade da decisão condenatória.

Art. 12º Perda de bens

1. O tribunal pode decretar a perda dos materiais, equipamentos ou dispositivos pertencentes à pessoa condenada que tiverem servido para a prática dos crimes previstos no presente diploma.

2. A perda de bens abrange o lucro ilícito obtido com a prática da infracção.

3. Se o tribunal apurar que o agente adquiriu determinados bens, empregando na sua aquisição dinheiro ou valores obtidos com a prática do crime, serão os mesmos também abrangidos pela decisão que decretar a perda.

Art. 13º Caução de boa conduta

1. A caução de boa conduta implica a obrigação de o agente depositar uma quantia em dinheiro, a fixar entre 10 000$ e 1 000 000$, à ordem do tribunal, pelo prazo fixado na decisão condenatória, por um período entre seis meses e dois anos.

2. A caução de boa conduta deve, em regra, ser aplicada sempre que o tribunal condene em pena cuja execução declare suspensa.

3. A caução será declarada perdida a favor do Estado se o agente praticar, por meio de informática, nova infracção no período fixado na sentença, pela qual venha a ser condenado, sendo-lhe restituída no caso contrário.

Art. 14º Interdição temporária do exercício de certas actividades ou profissões

1. A interdição temporária do exercício de certas actividades ou profissões pode ser decretada quando a infracção tiver sido cometida com flagrante e manifesto abuso da profissão ou no exercício de actividade que dependa de um título público ou de uma autorização ou homologação da autoridade pública.

2. A duração da interdição tem um mínimo de dois meses e um máximo de dois anos.

3. Incorre na pena do crime de desobediência qualificada quem, por si ou por interposta pessoa, exercer a profissão ou a actividade durante o período da interdição.

Art. 15º Encerramento temporário do estabelecimento

1. O encerramento temporário do estabelecimento pode ser decretado por um período mínimo de um mês e máximo de um ano, quando o agente tiver sido condenado em pena de prisão superior a 6 meses ou em pena de multa superior a 100 dias.

2. Não obstam à aplicação desta pena a transmissão do estabelecimento ou a cedência de direitos de qualquer natureza, relacionados com o exercício da profissão ou actividade, efectuados após a instauração do processo ou depois de cometida a infracção, salvo se, neste último caso, o adquirente se encontrar de boa-fé.

3. O encerramento do estabelecimento nos termos do nº 1 não constitui justa causa para o despedimento de trabalhadores nem fundamento para a suspensão ou redução do pagamento das respectivas remunerações.

Art. 16º Encerramento definitivo do estabelecimento

1. O encerramento definitivo do estabelecimento pode ser decretado quando o agente:

a) Tiver sido anteriormente condenado por infracção prevista neste diploma em pena de prisão ou multa, se as circunstâncias mostrarem que a condenação ou condenações anteriores não constituíram suficiente prevenção contra o crime;

b) Tiver anteriormente sido condenado em pena de encerramento temporário;

c) For condenado em pena de prisão por infracção prevista neste diploma, que tenha determinado dano de valor consideravelmente elevado ou para um número avultado de pessoas.

2. Aplicam-se ao encerramento definitivo as disposições dos nºs 2 e 3 do artigo anterior.

Art. 17º Publicidade da decisão

1. Quando o tribunal aplicar a pena de publicidade, será esta efectivada, a expensas do condenado, em publicação periódica editada na área da comarca da prática da infracção ou, na sua falta, em publicação da área da comarca mais próxima, bem como através da afixação de edital, por período não inferior a 30 dias, no próprio estabelecimento ou no local do exercício da actividade, por forma bem visível pelo público.

2. Em casos particularmente graves, nomeadamente quando a infracção importe lesão de interesses não circunscritos a determinada área do território, o tribunal poderá ordenar, também a expensas do condenado, que a publicidade da decisão seja feita no Diário da República ou através de qualquer meio de comunicação social.

3. A publicidade da decisão condenatória é feita por extracto, do qual constem os elementos da infracção e as sanções aplicáveis, bem como a identificação dos agentes.

CAPÍTULO IV - Disposições finais

Art. 18º Processo de liquidação

1. Transitada em julgado a decisão que aplicar a pena de dissolução, o Ministério Público requer a liquidação do património, observando-se, com as necessárias adaptações, o processo previsto na lei para a liquidação de patrimónios.

2. O processo de liquidação corre no tribunal da condenação e por apenso ao processo principal.

3. Os liquidatários são sempre nomeados pelo juiz.

4. O Ministério Público requer as providências cautelares que se mostrem necessárias para garantir a liquidação.

Art. 19º Entrada em vigor

O presente diploma entra em vigor no prazo de 120 dias a contar da sua publicação.

REINO UNIDO

http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm

Computer Misuse Act 1990 (c. 18)

1990 c. 18 - continued

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

[29th June 1990]

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Computer misuse offences

Unauthorised access to computer material.

1.—(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

Unauthorised access with intent to commit or facilitate commission of further offences.

2.—(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Unauthorised modification of computer material.

3.—(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in

any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Jurisdiction

Territorial scope of offences under this Act.

4.—(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at

least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

(4) Subject to section 8 below, where—

(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references—

(a) in the application of this Act to England and Wales, to England and Wales;

(b) in the application of this Act to Scotland, to Scotland; and

(c) in the application of this Act to Northern Ireland, to Northern Ireland.

Significant links with domestic jurisdiction.

5.—(1) The following provisions of this section apply for the interpretation of section 4 above.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.

(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification; or

(b) that the unauthorised modification took place in the home country concerned.

Territorial scope of inchoate offences related to offences under this Act.

6.—(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt—

(a) the question where any person became a party to the conspiracy; and

(b) the question whether any act, omission or other event occurred in the home country concerned.

(2) On a charge of attempting to commit an offence under section 3 above the following questions are immaterial to the accused's guilt—

(a) the question where the attempt was made; and

(b) the question whether it had an effect in the home country concerned.

(3) On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt.

(4) This section does not extend to Scotland.

Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.

7.—(1) The following subsections shall be inserted after subsection (1) of section 1 of the [1977 c. 45.] Criminal Law Act 1977—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an agreement, this Part of this Act has effect in relation to it as it has effect in relation to an agreement falling within subsection (1) above.

(1B) Subsection (1A) above applies to an agreement if—

(a) a party to it, or a party's agent, did anything in England and Wales in relation to it before its formation; or

(b) a party to it became a party in England and Wales (by joining it either in person or through an agent); or

(c) a party to it, or a party's agent, did or omitted anything in England and Wales in pursuance of it;

and the agreement would fall within subsection (1) above as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions."

(2) The following subsections shall be inserted after subsection (4) of that section—

"(5) In the application of this Part of this Act to an agreement to which subsection (1A) above applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in England and Wales.

(6) In this section "computer misuse offence" means an offence under the Computer Misuse Act 1990."

(3) The following subsections shall be inserted after section 1(1) of the [1981 c. 47.] Criminal Attempts Act 1981—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an act, what the person doing it had in view shall be treated as an offence to which this section applies.

(1B) Subsection (1A) above applies to an act if—

(a) it is done in England and Wales; and

(b) it would fall within subsection (1) above as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in England and Wales.

(4) Subject to section 8 below, if any act done by a person in England and Wales would amount to the offence of incitement to commit an offence under this Act but for the fact that what he had in view would not be an offence triable in England and Wales—

(a) what he had in view shall be treated as an offence under this Act for the purposes of any charge of incitement brought in respect of that act; and

(b) any such charge shall accordingly be triable in England and Wales.

Relevance of external law.

8.—(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) A person is guilty of an offence triable by virtue of section 1(1A) of the [1977 c. 45.] Criminal Law Act 1977 only if the pursuit of the agreed course of conduct would at some stage involve—

(a) an act or omission by one or more of the parties; or

(b) the happening of some other event;

constituting an offence under the law in force where the act, omission or other event was intended to take place.

(3) A person is guilty of an offence triable by virtue of section 1(1A) of the [1981 c. 47.] Criminal Attempts Act 1981 or by virtue of section 7(4) above only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(5) Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice—

(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to show that it is satisfied.

(6) In subsection (5) above "the relevant conduct" means—

(a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;

(b) where the condition in subsection (2) above is in question, the agreed course of conduct; and

(c) where the condition in subsection (3) above is in question, what the accused had in view.

(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.

(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.

(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.

(10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.

British citizenship immaterial.

9.—(1) In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

(2) This section applies to the following offences—

(a) any offence under this Act;

(b) conspiracy to commit an offence under this Act;

(c) any attempt to commit an offence under section 3 above; and

(d) incitement to commit an offence under this Act.

Miscellaneous and general

Saving for certain law enforcement powers.

10. Section 1(1) above has effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.

Proceedings for offences under section 1.

11.—(1) A magistrates' court shall have jurisdiction to try an offence under section 1 above if—

(a) the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time.

(2) Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge.

(3) No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.

(4) For the purposes of this section, a certificate signed by or on behalf of the prosecutor and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(5) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(6) In this section "commission area" has the same meaning as in the Justices of the [1979 c. 55.] Peace Act 1979.

(7) This section does not extend to Scotland.

Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.

12.—(1) If on the trial on indictment of a person charged with—

(a) an offence under section 2 above; or

(b) an offence under section 3 above or any attempt to commit such an offence;

the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.

(2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 1 above as a magistrates' court would have on convicting him of the offence.

(3) This section is without prejudice to section 6(3) of the [1967 c. 58.]

Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment).

(4) This section does not extend to Scotland.

Proceedings in Scotland.

13.—(1) A sheriff shall have jurisdiction in respect of an offence under section 1 or 2 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the sheriffdom at that time.

(2) A sheriff shall have jurisdiction in respect of an offence under section 3 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the unauthorised modification; or

(b) the unauthorised modification took place in the sheriffdom.

(3) Subject to subsection (4) below, summary proceedings for an offence under section 1, 2 or 3 above may be commenced within a period of six months from the date on which evidence sufficient in the opinion of the procurator fiscal to warrant proceedings came to his knowledge.

(4) No such proceedings shall be commenced by virtue of this section more than three years after the commission of the offence.

(5) For the purposes of this section, a certificate signed by or on behalf of the procurator fiscal and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.

(6) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.

(7) Subsection (3) of section 331 of the [1975 c. 21.] Criminal Procedure (Scotland) Act 1975 (date of commencement of proceedings) shall apply for the purposes of this section as it applies for the purposes of that section.

(8) In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence commenced before the expiry of any time

limit under this section applicable to such proceedings.

(9) Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.

(10) A person found guilty of an offence under section 1 above by virtue of subsection (8) above shall be liable, in respect of that offence, only to the penalties set out in section 1.

(11) This section extends to Scotland only.

Search warrants for offences under section 1.

14.—(1) Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing—

(a) that an offence under section 1 above has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises;

he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.

(2) The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in section 9(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 (privileged, excluded and special procedure material).

(3) A warrant under this section—

(a) may authorise persons to accompany any constable executing the warrant; and

(b) remains in force for twenty-eight days from the date of its issue.

(4) In executing a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.

(5) In this section "premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.

(6) This section does not extend to Scotland.

Extradition where Schedule 1 to the Extradition Act 1989 applies.

15. The offences to which an Order in Council under section 2 of the [1870 c. 52.] Extradition Act 1870 can apply shall include—

(a) offences under section 2 or 3 above;

(b) any conspiracy to commit such an offence; and

(c) any attempt to commit an offence under section 3 above.

Application to Northern Ireland.

16.—(1) The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned.

(2) In section 2(2)(b)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the [S.I. 1981/1675 (N.I.26).] Magistrates' Courts (Northern Ireland) Order 1981.

(3) The reference in section 3(6) to the [1971 c. 48.] Criminal Damage Act 1971 shall be read as a reference to the [S.I. 1977/426 (N.I.4).] Criminal Damage (Northern Ireland) Order 1977.

(4) Subsections (5) to (7) below apply in substitution for subsections (1) to (3) of section 7; and any reference in subsection (4) of that section to England and Wales shall be read as a reference to Northern Ireland.

(5) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the [S.I. 1983/1120 (N.I.13).] Criminal Attempts and Conspiracy (Northern Ireland) Order 1983—

"(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

(1B) Paragraph (1A) applies to an agreement if—

(a) a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;

(b) a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or

(c) a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;

and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions."

(6) The following paragraph shall be inserted after paragraph (4) of that Article—

application of this Part to an agreement to which

Interpretation.

17.—(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if—

(a) the person whose act causes it is not himself entitled to *determine whether* the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

Citation, commencement etc.

18.—(1) This Act may be cited as the Computer Misuse Act 1990.

(2) This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.

(3) An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.

SUÉCIA

http://wings.buffalo.edu/law/bclc/sweden.pdf

The Penal Code

Chapter 4 - On Crimes against Liberty and Peace

Section 9c

A person who, in cases other than those defined in Sections 8 and 9,unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years. A recording in this context includes even information that is being

processed by electronic or.similar means for use with automatic data processing. (Law1998:206)

SUíÇA

http://www.admin.ch/ch/f/rs/3/311.0.fr.pdf

Code pénal suisse
du 21 décembre 1937 (Etat le 5 décembre 2000)

Art. 143 bis Accès indu à un système informatique - Celui qui, sans dessein d'enrichissement, se sera introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part, sera, sur plainte, puni de l'emprisonnement ou de l'amende.

ANEXO B

Projetos Legislativos

Brasil:

PROJETO DE LEI Nº 84 DE 1999

(Do Sr. Luiz Piauhylino)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇAO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º - *O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.*

Art. 2º - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.

Art. 3º - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º - Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º - A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tomada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta.

§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§ 4º. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º - Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º - O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I
Dano a dado ou programa de computador

Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. *Se* o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II- com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro , ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa.

Seção II
Acesso indevido ou não autorizado

Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV
Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11 - Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V

Violação de segredo armazenado em computador, meio magnético ,

de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programa de computador c nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra a interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevid6 de senha ou processo de Identificação de terceiro; ou

VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia através de rede de computadores

Art. 14 - Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

CAPITULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15 - Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16 - Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 17 - Esta lei regula os crimes relativos à informática sem prejuízo das demais comunicações previstas em outros diplomas legais.

Art 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

JUSTIFICAÇÃO

Na legislatura passada o ilustre Deputado Cássio Cunha Lima apresentou o PL 1.713196 que dispõe sobre o acesso, a responsabilidade e os crimes cometido nas redes integradas de computadores. Na justificativa do nobre Deputado, houve a preocupação com a informação dessas redes de computadores em verdadeiros mercados, no sentido econômico da palavra, onde pessoas conversam, trocam informações e realizam transações comerciais, não existindo porém nenhuma legislação específica que regule as responsabilidade dos agentes envolvidos.

Distribuído inicialmente à Comissão de Ciência e Tecnologia, Comunicação e Informática, o PL 1.713/96 foi encaminhado a minha pessoa para ser o Relator do mesmo. Iniciei a discussão na comissão, inclusive com convocação de audiência publica e, em seguida com pessoas da área de informática, buscando identificar um texto que tratasse a matéria de uma forma mais global. Sob a coordenação do professor José Henrique Barbosa Moreira Lima Neto formou-se um, grupo composto dos seguintes membros:

- Dr. Damásio Evangelista de Jesus, advogado(SP)
- Dr. Gilberto Martins de Almeida, advogado (RJ)
- Dr. Ivan Lira de Carvalho, Juiz Federal (RN)
- Dr. Mário César Monteiro Machado, Juiz Auditor Militar (RJ) - Dr. Carlos Alberto Etcheverry, Juiz de Direito (RS)
- Dr. Júlio César Finger, Promotor de Justiça (RS)
- Dra. Marília Cohen Goldman, Promotora de Justiça (RS)
- Dra. Lígia Leindecker Futterrleib, advogada (RS)
- Dr. Paulo Sérgio Fabião, Desembargador (RJ).

Este grupo, depois de vários debates "on-line" apresentou-me urna minuta do substitutivo ao referido PL 1.713196. Ocorre que, por falta de tempo suficiente o substitutivo não foi devidamente apreciado, inclusive pelas demais comissões da Câmara dos Deputados, durante a legislatura passada, razão pela qual o PL foi arquivado. Portanto apresento agora o PL acima , o qual é resultado de um trabalho sério, depois de ouvir a sociedade, através de pessoas da mais alta qualificação.

Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para

propósitos escusos e criminosos. Dai a necessidade de uma lei que, defina os crimes cometidos na rede de informática e suas respectivas penas.

Sala das Sessões, em de de 1.999.

Deputado LUIZ PIAUHYLINO
PSDB/PE

Europa

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

FINAL ACTIVITY REPORT

Prepared by : Committee of Experts on Crime in Cyber-Space (PC-CY)

Approved by : European Committee on Crime Problems (CDPC) at its 50th plenary session
(18 - 22 June 2001)

DRAFT CONVENTION ON CYBER-CRIME

Introductory Note
for the attention of the Committee of Ministers

The European Committee on Crime Problems (CDPC) carefully examined the objections formulated by some delegations against the federal clause contained in Article 41 of the draft convention. The inclusion of such a clause involves a delicate balance between different values of the international legal order.

In order to take into account these objections, the CDPC decided to introduce the following amendments to the draft convention with a view to restricting the application of the clause as much as possible:

- The scope of application has been restricted to the provisions of Chapter II (substantive criminal law, procedural law and jurisdiction). Federal States making use of this provision would still be under the obligation to co-operate fully with the other Parties under Chapter III.

- A new paragraph was added to the clause requiring the federal government to refer the provisions, the implementation of which come under the jurisdiction of constituent states or other similar territorial entities, to the authorities of such entities with a favourable opinion.

- Article 46 of the draft convention on multilateral consultations of the Parties was complemented. The Parties will be required to examine regularly the effects of reservations and declarations, including federal declarations, on the Convention's operation.

- Article 37 of the draft convention has been strengthened. It now provides that acceding federal States which intend to use the federal clause are required to submit in advance a draft of the statement required under Article 41(3) so that Contracting Parties will be in a position to evaluate how application of the Federal clause would affect the prospective Party's implementation of the Convention.

The CDPC is convinced that with these amendments the federal clause in this Convention accommodates the internal difficulties federal States may face as a result of their characteristic distribution of powers between central and regional authorities, while not unduly impairing the principle of parity of treaty obligations. Three delegations (France, Andorra and Greece), however, maintained their objections against the federal clause; as concerns France, as a matter of legal principle and because it would create a precedent in international conventions on criminal law. The U.S. delegation reiterated its position that the absence of a federal clause would raise significant and fundamental legal and policy concerns creating obstacles to the United States becoming a Party to the Convention.

At this point, the decision about the inclusion of the federal clause is no longer a purely technical issue, to be decided by the legal experts. The matter will therefore have to be decided by the Committee of Ministers. As this Convention is a legal instrument negotiated by sovereign States, the observer States represented in the CDPC declared that they wished to be represented at the meeting of the Committee of Ministers that adopts the Convention.

DRAFT CONVENTION ON CYBER-CRIME

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States signatories to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cyber-crime, *inter alia* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cyber-crime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cyber-crime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cyber-crimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, Recommendation N° R (88) 2 on piracy in the field of copyright and neighbouring rights, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services as well as Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3 adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to

the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cyber-crime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;

2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention with intent that such offence be committed.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1) a and 9 (1) c of this Convention.

3. Each State may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a legal person can be held liable for a criminal offence established in accordance with this Convention, committed for its benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a. the criminal offences established in accordance with articles 2-11 of this Convention;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

3. a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b. Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to

communications being transmitted within a computer system of a service provider, which system

i. is being operated for the benefit of a closed group of users, and

ii. does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 - Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

3. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control;

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:

a. the type of the communication service used, the technical provisions taken thereto and the period of service;

b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. a computer system or part of it and computer data stored therein; and

b. computer-data storage medium in which computer data may be stored,

in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or

2. These measures shall include the power to :

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. make and retain a copy of those computer data;

c. maintain the integrity of the relevant stored computer data; and

c. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a), it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data of specified communications in its territory through application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed :

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each State may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1. a. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7. a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 - 35.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in Articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1. A Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2. Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 10 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. a. Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other.

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.

4. The requested Party may, in addition to grounds for refusal available under Article 25, paragraph (4), refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9. a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation, is available unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2. The requested Party may make the furnishing of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information is nevertheless provided. When the requesting Party accepts the condition, it shall be bound by it.

4. Any Party that furnishes information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

a. the authority that is seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceeding and a brief summary of related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information to identify the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data may, in respect of offences other than those established in accordance with Articles 2 – 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; *or*

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 60 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if :

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this Chapter.

3. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without obtaining the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system. Subject to paragraph 2, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted by their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a. provision of technical advice;

b. preservation of data pursuant to Articles 29 and 30; and

c. collection of evidence, giving of legal information, and locating of suspects.

2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20 (d) of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

[3. Any State seeking to accede to the present Convention, which intends to make a declaration under Article 41, shall provide to the Secretary General the proposed statement referred to in that Article. The Secretary General shall submit such a proposed statement to the Contracting States and other States entitled to sit on the Committee of Ministers prior to the decision being taken under paragraph 1 above.]

Article 38 – Territorial application

1. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1. The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition opened for signature in Strasbourg on 13 December 1957 (ETS No. 24);

- the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 20 April 1959 (ETS No. 30);

- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise have established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Article 2, Article 3, Article 6, paragraph 1 (b), Article 7, Article 9, paragraph 3 and Article 27, paragraph 9 (e).

[Article 41 – Federal clause

1. A federal State may notify the Secretary General at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, that it shall assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2. With regard to the provisions of this Convention, the implementation of which come under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion.

3. When making a declaration under paragraph 1, a federal State shall provide a statement regarding the nature of its federal system, and of the effect of its federal character on the implementation of the Convention.] (1)

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4,

paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1. A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2. A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3. The Secretary General may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the European Committee on Crime Problems (CDPC) and, following consultation with the non-member State Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cyber-crime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The European Committee on Crime Problems (CDPC) shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this Article.

Article 47 – Denunciation

1. Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance, approval or accession;

c. any date of entry into force of this Convention in accordance with Articles 36 and 37;

d. any declaration made under Article[s] 40 [and 41] or reservation made in accordance with Article 42;

e. any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

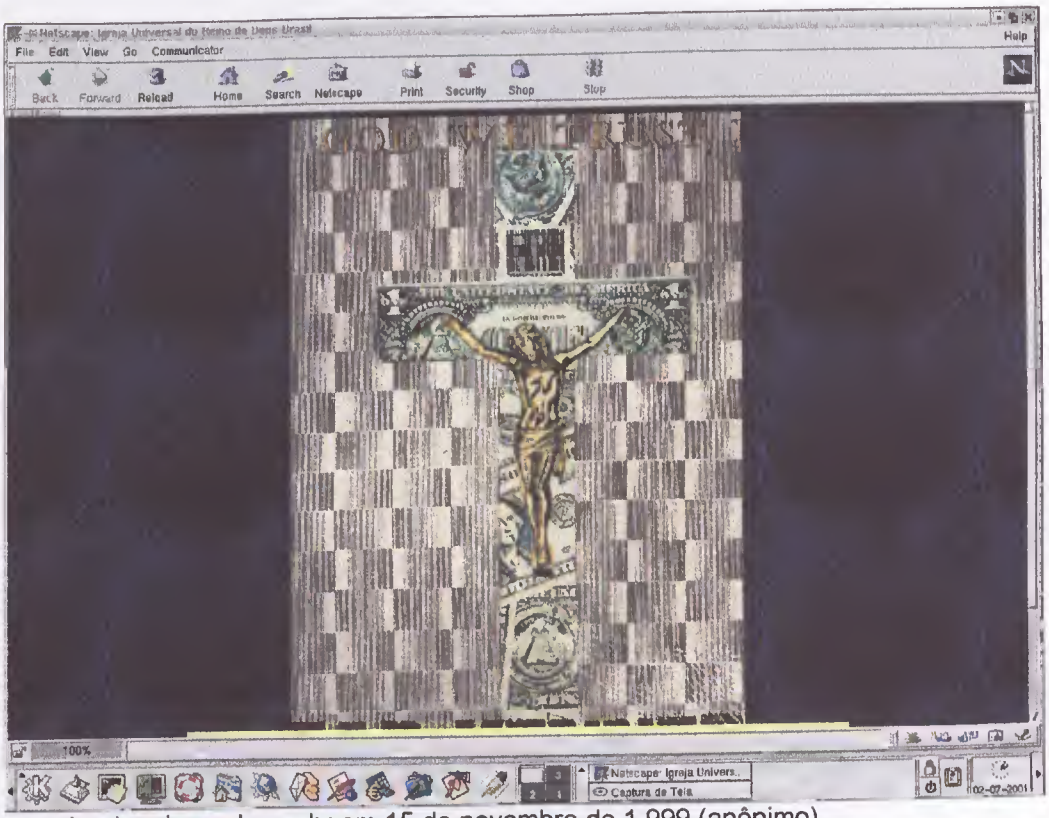
Done at Strasbourg, on .... 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Note :

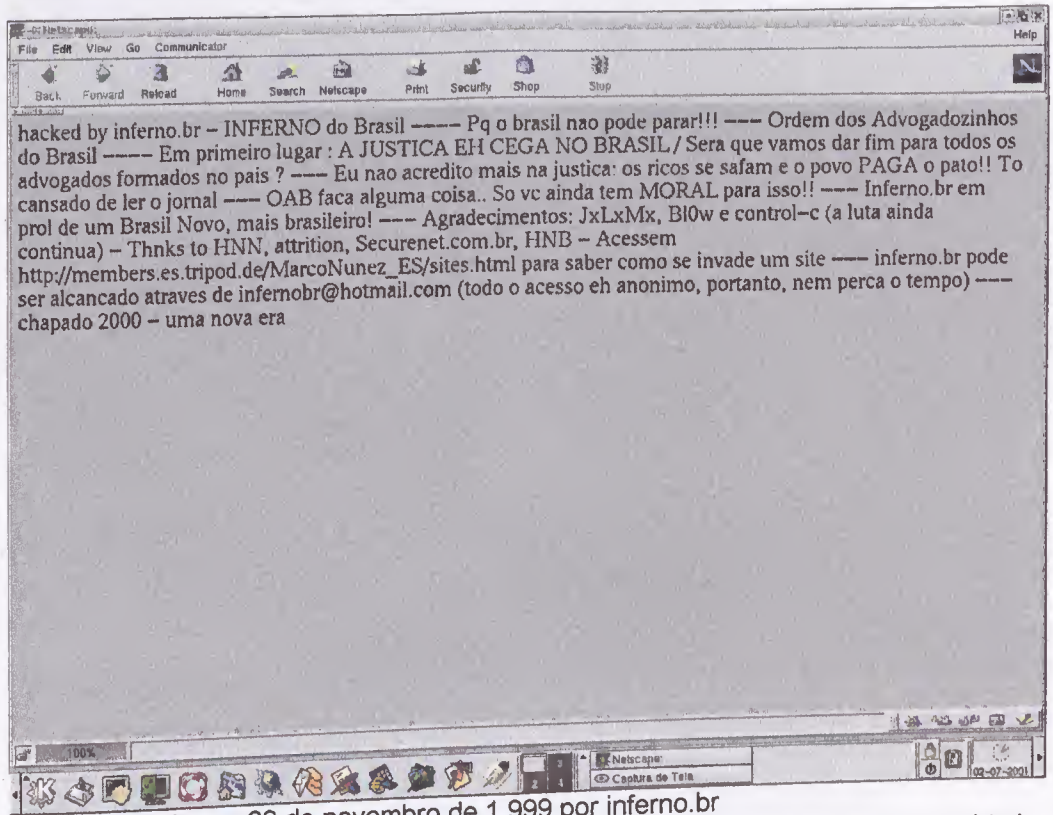
(1) See the Introductory Statement submitted by the CDPC to the Committee of Ministers on this issue. Back.

ANEXO C

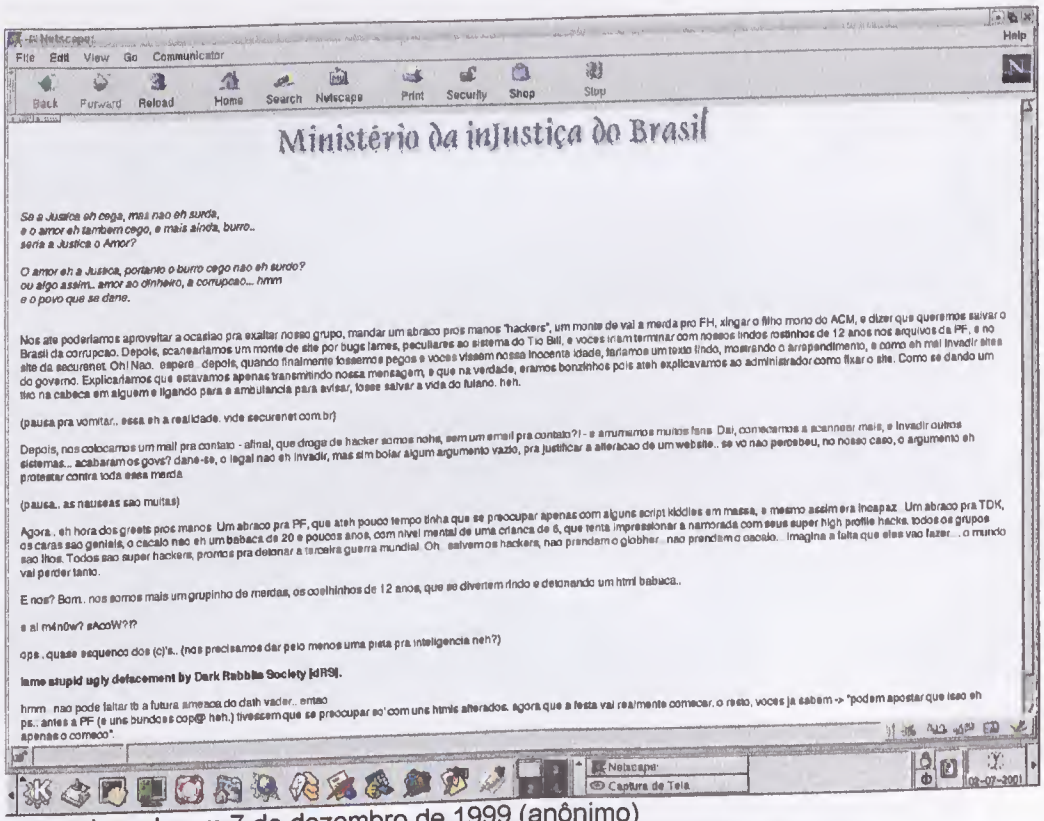
Páginas Transfiguradas



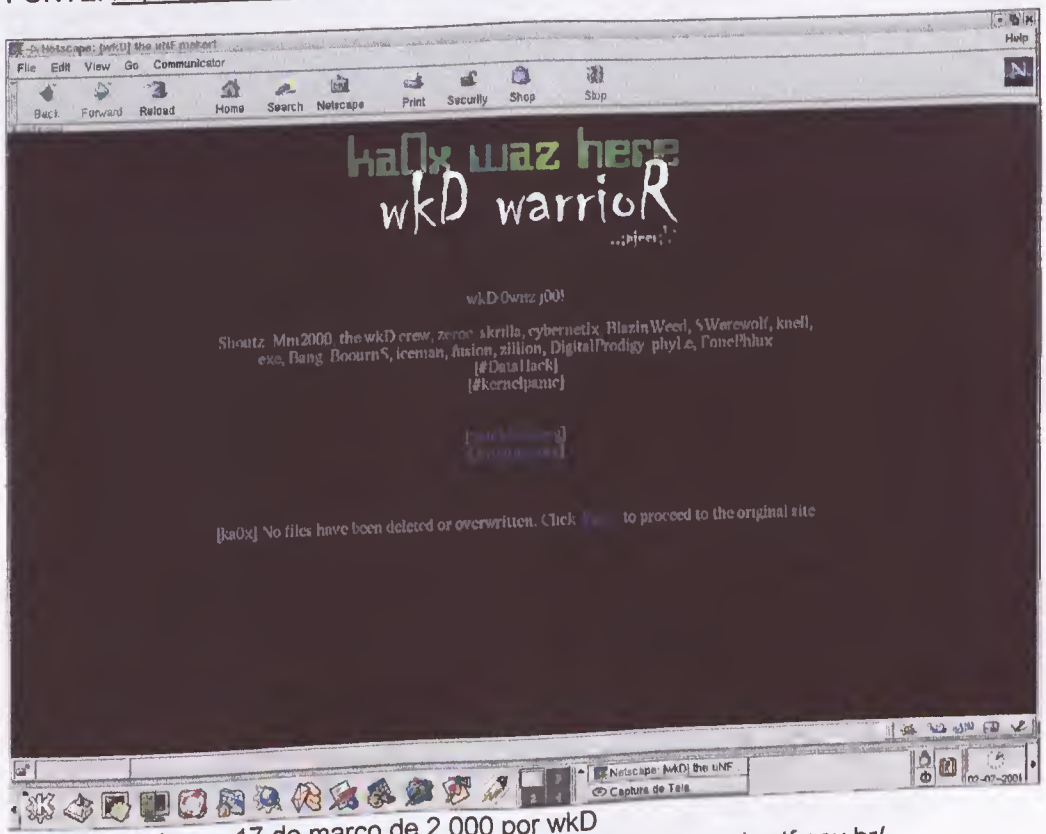
www.igrejauniversal.com.br em 15 de novembro de 1.999 (anônimo)
FONTE: http://www.attrition.org/mirror/attrition/1999/11/15/www.igrejauniversal.com.br/



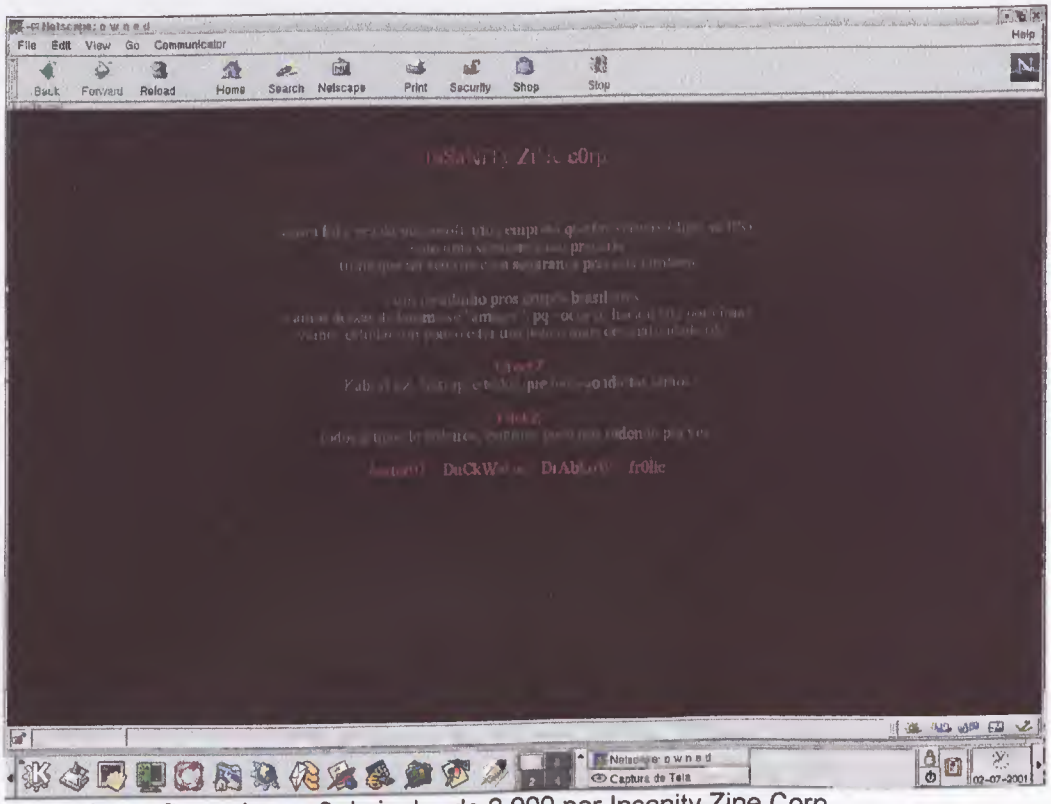
www.oab.org.br em 29 de novembro de 1.999 por inferno.br
FONTE: http://www.attrition.org/mirror/attrition/1999/11/29/www.oab.org.br/mirror.html



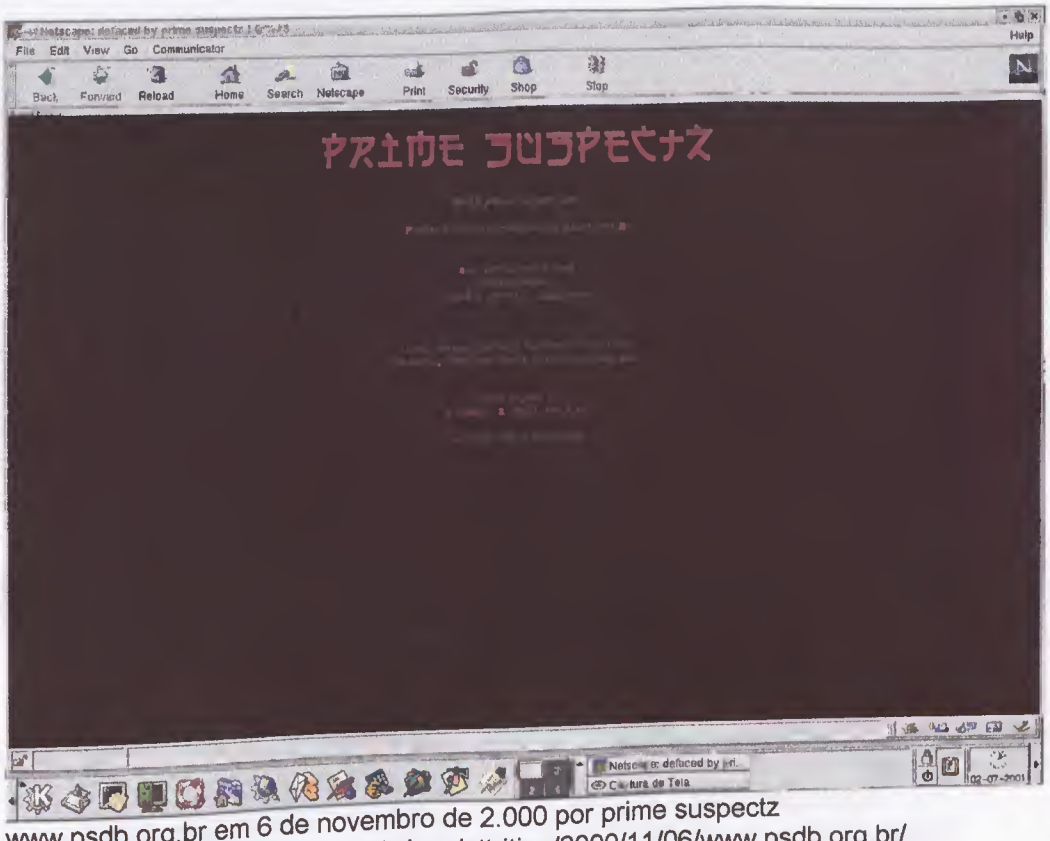
www.mj.gov.br em 7 de dezembro de 1999 (anônimo)
FONTE: http://www.attrition.org/mirror/attrition/1999/12/07/www.mj.gov.br/



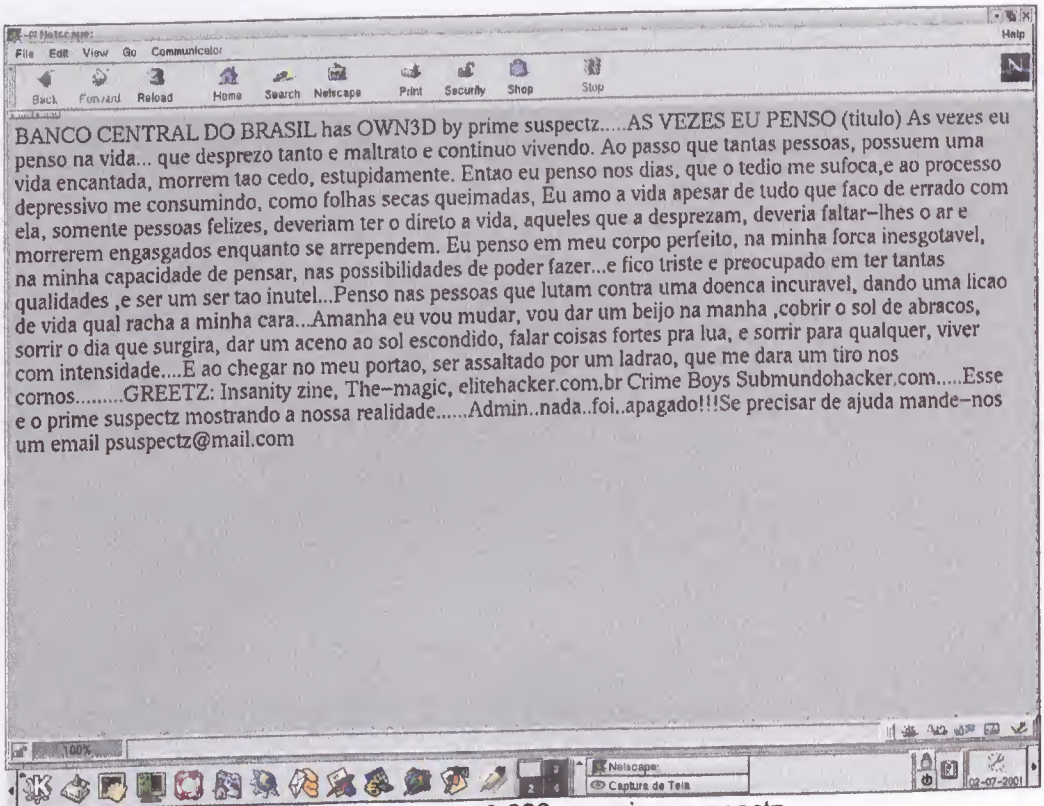
www.stf.gov.br em 17 de março de 2.000 por wkD
FONTE: http://www.attrition.org/mirror/attrition/2000/03/17/pyxis.stf.gov.br/



www.microsoft.com.br em 3 de junho de 2.000 por Insanity Zine Corp
FONTE: http://www.attrition.org/mirror/attrition/2000/06/03/www.microsoft.com.br/

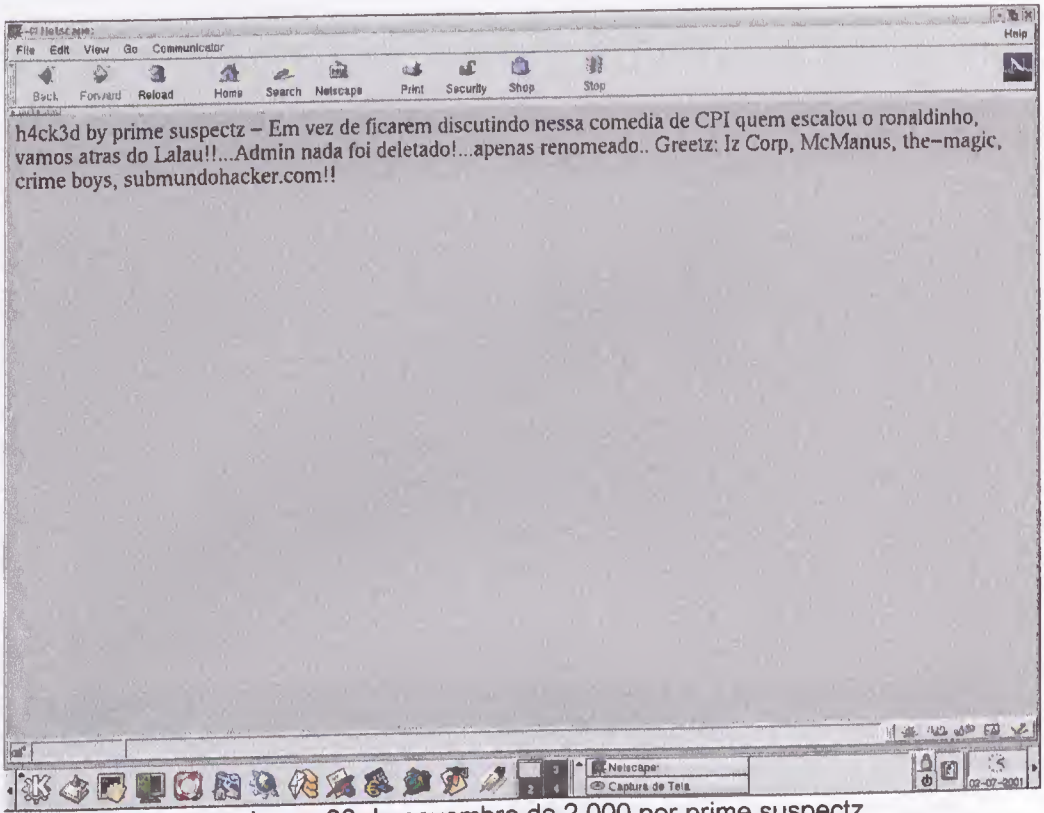


www.psdb.org.br em 6 de novembro de 2.000 por prime suspectz
FONTE: http://www.attrition.org/mirror/attrition/2000/11/06/www.psdb.org.br/

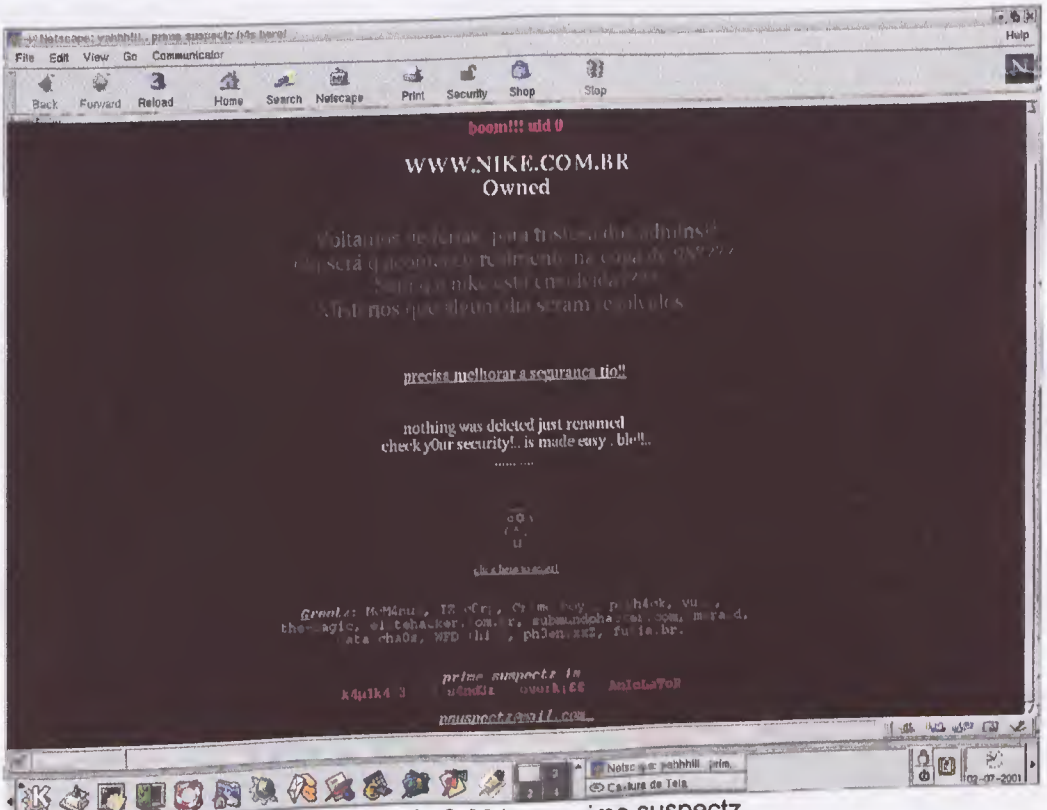


www.bcb.gov.br em 27 de novembro de 2.000 por prime suspectz
FONTE: http://www.attrition.org/mirror/attrition/2000/11/27/www.bcb.gov.br/mirror.html

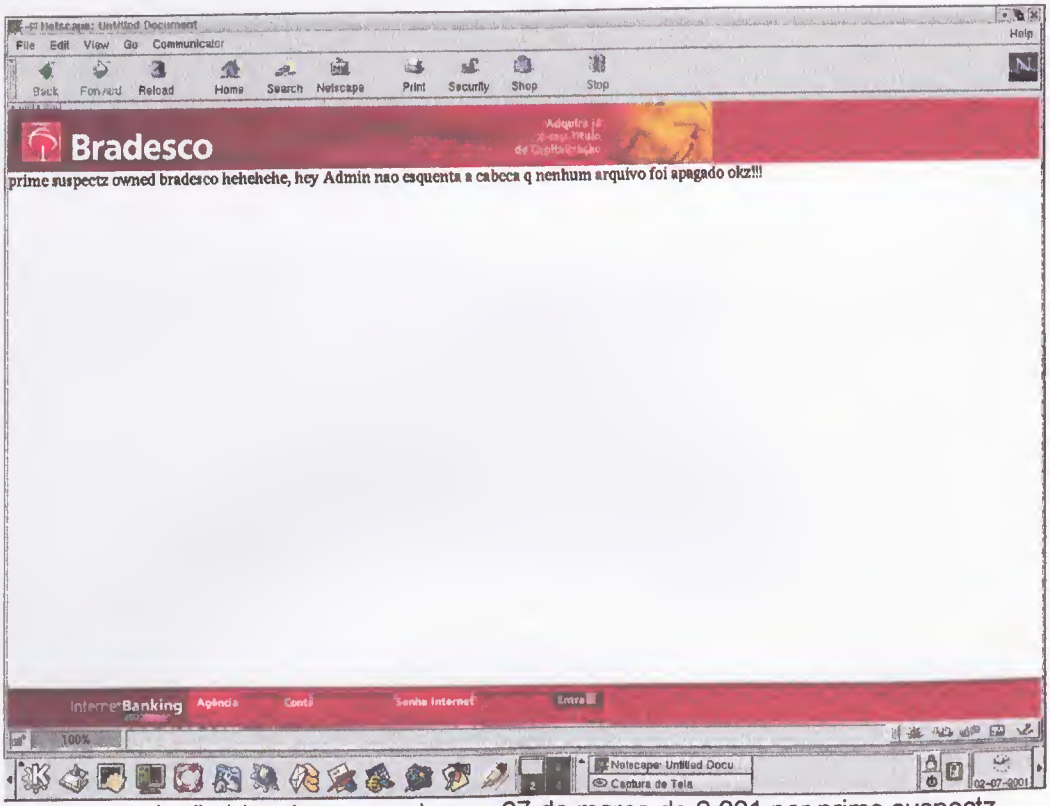
www.mcafee.com.br em 29 de novembro de 2.000 por Insanity Zine Corp
FONTE: http://www.attrition.org/mirror/attrition/2000/11/29/www.mcafee.com.br/



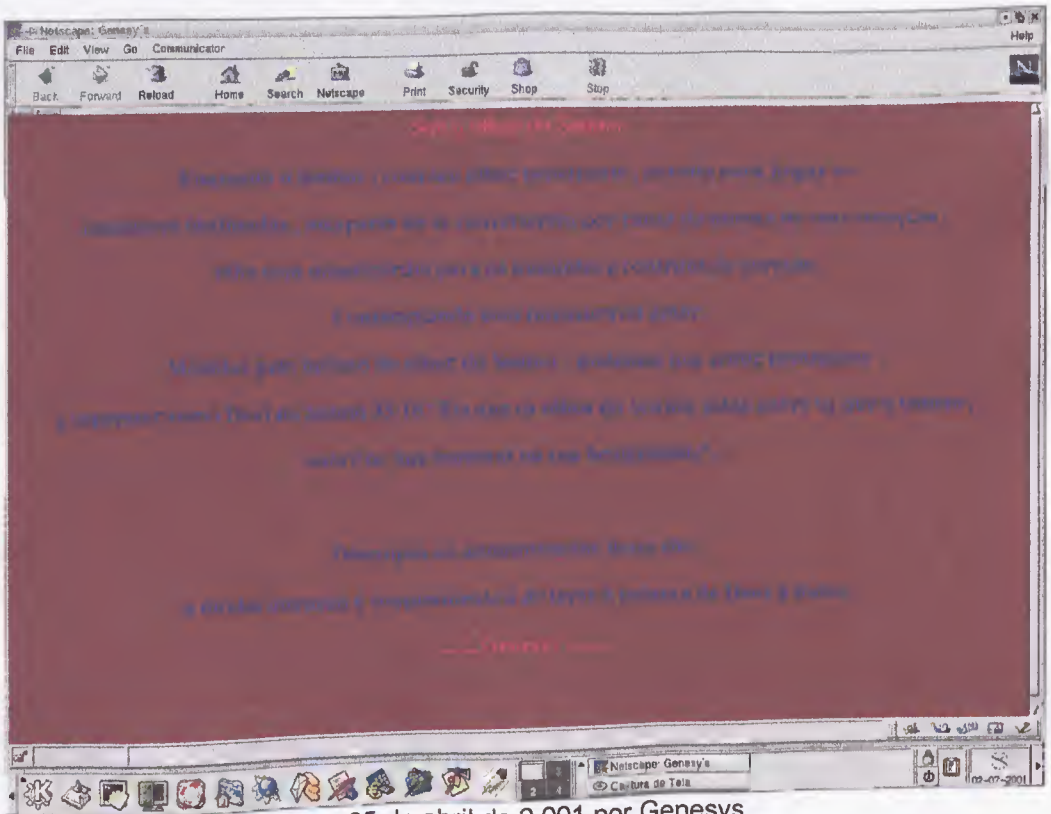
www.congresso.gov.br em 30 de novembro de 2.000 por prime suspectz
FONTE: http://www.attrition.org/mirror/attrition/2000/11/30/www.congresso.gov.br/



www.nike.com.br em 7 de janeiro de 2.001 por prime suspectz
FONTE: http://www.attrition.org/mirror/attrition/2001/01/07/www.nike.com.br/



www.preprodução1.bradesco.com.br em 27 de março de 2.001 por prime suspectz
FONTE:
http://www.attrition.org/mirror/attrition/2001/03/27/www.preproducao1.bradesco.com.br/



www.mcdonalds.com.br em 25 de abril de 2.001 por Genesys
FONTE: http://www.attrition.org/mirror/attrition/2001/04/25/www.mcdonalds.com.br/

ANEXO D

CD-ROM

ANEXO D

CD-ROM