MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA DA REPÚBLICA NO ESTADO DE SP
GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS

MANUAL PRÁTICO DE INVESTIGAÇÃO

ABRIL DE 2006

REDAÇÃO: Adriana Shimabukuro Kurokawa (técnica em informática – PR-SP), Sergio Gardenghi Suiama, Ana Carolina Previtalli Nascimento, Karen Louise Jeanette Kahn e Eduardo Barragan Serôa da Motta (Procuradores da República)

REVISÃO TÉCNICA: Thiago Tavares Nunes de Oliveira, Carla Elaine Freitas, Thiago Oliveira Castro Vieira e Moisés Araújo Machado (Safernet Brasil)

REVISÃO FINAL: Sergio Gardenghi Suiama e Adriana Shimabukuro Kurokawa

GRUPO DE CRIMES CIBERNÉTICOS DA PR-SP: Ana Letícia Absy, Anamara Osório Silva de Sordi, Karen Louise Jeanette Kahn, Sergio Gardenghi Suiama e Thaméa Danelon Valiengo (Procuradores da República), Adriana Shimabukuro Kurokawa (consultora técnica), Fernando Jesus Conceição e Ipólito Francisco Jorge.

PROCURADORA CHEFE: Adriana Zawada Melo

AGRADECIMENTOS: ao Comitê Gestor da Internet no Brasil, a António Alberto Valente Tavares, a Thiago Tavares Nunes de Oliveira e equipe do Safernet Brasil, a Anderson e Roseane Miranda (do *hotline* censura.com.br*)*, a Suely Freitas da Silva e aos ex-estagiários da PR-SP Patrícia Cotrim e Marcelo Chiara Teixeira.

PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO
Rua Peixoto Gomide, 768 – Cerqueira César
CEP 01409-904 – São Paulo – SP
Telefone: (11) 3269-5000
Home-page: www.prsp.mpf.gov.br

ÍNDICE

1. APRESENTAÇÃO.

Este manual nasceu de uma necessidade: em meados de 2002, um grupo de Procuradores da República decidiu pedir à Associação Brasileira Multiprofissional de Proteção à Infância e à Adolescência – ABRAPIA que as notícias de *sites* contendo fotografias ou imagens de pornografia infantil fossem encaminhadas diretamente ao Ministério Público Federal para que pudéssemos investigar, de maneira eficaz, essa conduta criminosa.

Recebemos daquela organização não-governamental dezenas de endereços de *sites* sediados no Brasil e no exterior, e, naquele momento, percebemos nossa total ignorância a respeito dos meandros da criminalidade cibernética; um mundo quase inacessível para quem, como nós, nasceu no tempo das máquinas de escrever e não sabia nem mesmo o que era um *browser*.

Bem, segundo um antigo provérbio latino, a necessidade é a mãe da invenção. O número de investigações relacionadas a crimes cibernéticos é crescente, e é razoável supor que, à medida que novos usuários ingressem na rede e mais pessoas passem a ter o domínio das estruturas básicas do sistema, surjam formas de criminalidade informática para as quais não temos nenhum conhecimento. Foi preciso, então, começar um processo de formação, do qual este manual é apenas um primeiro modesto resultado.

Nosso objetivo com a publicação é dividir com os profissionais do direito que participam de algum modo da atividade de persecução penal (delegados, membros do Ministério Público, juízes e auxiliares da Justiça) os conhecimentos que o grupo de combate aos crimes cibernéticos da PR-SP acumulou até agora, apresentando os procedimentos básicos de coleta, preservação da integridade e análise das provas e de identificação dos autores desses crimes. Como os assuntos aqui tratados dizem respeito a técnicas de investigação, é desnecessário lembrar a inconveniência de divulgação mais ampla do manual.

O tema da criminalidade cibernética é por demais extenso e as novas tecnologias que surgem a cada dia desafiam os conhecimentos acumulados no presente. Por isso, nossas pretensões com o manual são bastante modestas e se dirigem, principalmente, ao combate dos principais crimes praticados por intermédio da rede mundial de computadores de competência da Justiça Federal brasileira, notadamente a pornografia infantil e os chamados “crimes de ódio” (*hate crimes*).

Temos plena convicção de que a efetividade da aplicação da lei penal em relação a esses crimes depende da aquisição de conhecimentos mínimos de informática pelos operadores do direito. Depende, também, de uma postura menos burocrática de nossa parte, já que o tempo da Internet é muitíssimo mais rápido do que o tempo dos órgãos envolvidos na persecução penal. Basta lembrar, a propósito, que a maioria dos provedores de acesso à Internet no Brasil guarda as informações necessárias à investigação dos crimes cibernéticos por apenas três ou quatro meses, em

razão do grande espaço de memória exigido para o armazenamento dessas informações.

Agradecemos muitíssimo o Comitê Gestor da Internet no Brasil, nas pessoas de Demi Getschko e Hartmut Richard Glaser e o presidente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet – ABRANET, António Alberto Valente Tavares, pelo apoio e patrocínio da publicação desta obra.

Agradecemos também as Procuradoras-Chefes da Procuradoria da República em São Paulo Elizabeth Mitiko Kobayashi e Adriana Zawada Melo, por terem determinado o suporte necessário às iniciativas desenvolvidas pelo grupo.

Aqueles que começam a trabalhar com o assunto cedo percebem as imensas limitações que encontramos para combater a disseminação, na rede mundial de computadores, da pornografia infantil, do racismo, e de outros crimes com alto potencial lesivo. O caráter transnacional do delito, a extrema volatilidade das evidências e o despreparo do sistema de justiça para lidar com essa forma de criminalidade são os principais fatores de insucesso das investigações. Temos consciência de todos esses problemas, e achamos que é hora de compartilhar conhecimentos e multiplicar o número de profissionais preparados para enfrentar a questão. Esperamos que a leitura do manual seja de alguma forma útil. E, desde já, colocamo-nos inteiramente à disposição dos colegas para ajudar no que for preciso. Mãos à obra!

2. COMO FUNCIONA A INTERNET?

No ano de 1962, em pleno auge da Guerra Fria, um grupo de pesquisadores americanos vinculados a uma instituição militar começou a imaginar um sistema imune a bombardeios, que fosse capaz de interligar muitos computadores, permitindo o intercâmbio e o compartilhamento de dados entre eles. Sete anos mais tarde, a primeira versão desse sistema ficou pronta: chamava-se ARPAnet (nome derivado de *Advanced Research Projects Agency* ou Agência de Projetos de Pesquisa Avançada), e sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando.

O nome "Internet" surgiu décadas mais tarde, quando a tecnologia desenvolvida passou a ser usada para ligar universidades americanas entre si, e depois também institutos de pesquisa sediados em outros países. A idéia central, porém, permaneceu a mesma: uma espécie de *associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erros em comunicação de dados*. Esse conjunto de regras recebeu a denominação de **protocolo**.

A exploração comercial do serviço começou no início da década de 90 e se desenvolveu graças à invenção da *World Wide Web*, um enorme pacote de informações, em formato de texto ou mídia (imagens e arquivos de áudio e vídeo), organizadas de forma a que o usuário possa percorrer as páginas na rede (isto é, "navegar"), a partir de seqüências associativas (*links*) entre blocos vinculados por remissões.

Do início da década de 90 até o presente, o número de usuários da Internet explodiu. Em 1990, havia cerca de 2 milhões de pessoas conectadas à rede em todo o mundo. Doze anos mais tarde, esse número passou para 604 milhões (cf. tabela 1). No Brasil, estima-se que o número de usuários da Internet seja de 14,3 milhões.

Tabela 1: Número de usuários da Internet no mundo:

	País	Usuários da Internet	Data da Informação
1	**Estados Unidos**	159,000,000	2002
2	**China**	59,100,000	2002
3	**Japão**	57,200,000	2002
4	**Alemanha**	34,000,000	2002
5	**Coréia do Sul**	26,270,000	2002
6	**Reino Unido**	25,000,000	2002
7	**Itália**	19,900,000	2002
8	**França**	18,716,000	2002
9	**Índia**	16,580,000	2002

10	**Canadá**	16,110,000	2002
11	**Brasil**	14,300,000	2002
12	**México**	10,033,000	2002
13	**Austrália**	9,472,000	2002
14	**Polônia**	8,880,000	2002
15	**Taiwan**	8,590,000	2002
16	**Holanda**	8,200,000	2002
17	**Indonésia**	8,000,000	2002
18	**Malásia**	7,841,000	2002
19	**Espanha**	7,388,000	2001
	Mundo	604,111,719	

Fonte: The Cia's World Factbook

Em geral, as informações na *Web* estão agrupadas em *sites*, que são coleções de páginas a respeito de um determinado assunto. Há, hoje, aproximadamente 800 milhões de *sites* publicados na rede. Todos eles podem ser acessados por intermédio de programas de navegação (*browsers*) como o *Internet Explorer,* o *Netscape* ou o *Mozilla Firefox*. O "endereço" que digitamos nesses programas de navegação para acessar algum *site* (por exemplo, www.stf.gov.br) é chamado de **URL**, abreviação de *Uniform Resource Locator*, ou "*Localizador Uniforme de Recursos*".

Os endereços da *Web* seguem uma estrutura ordenada, composta por **domínios**. No URL do Supremo Tribunal Federal, por exemplo, após a sigla www, há o nome do *site* (".stf"), um sufixo que indica o tipo de organização (no caso, ".gov"), e duas letras finais para designar o país de origem (".br"). Essas três partes que compõem o endereço eletrônico receberam, respectivamente, a denominação de "nomes de domínio" ou *domain names* (como "google", "yahoo", "uol", "globo")[1]; "domínios de nível superior" (".gov", ".com", ".edu", ".org" etc.); e "domínios de países" (.br, .fr., .it, .pt etc.). *Sites* sediados nos Estados Unidos não possuem a extensão final porque, no princípio, a *Web* estava restrita àquele país e não se julgou necessário acrescentar o domínio específico.

Os URLs que digitamos nos programas de navegação precisam ser "traduzidos" para um endereço numérico, denominado **"endereço IP"**. Dissemos mais acima que as comunicações entre os computadores conectados à rede são feitas por intermédio de regras padronizadas, chamadas de "protocolos". Pois bem, a abreviação "IP" refere-se justamente a esses protocolos da Internet. Cada *site* ou página que acessamos está hospedado em um computador permanentemente ligado à rede, chamado de *servidor*, o qual é identificado apenas pelo endereço numérico IP. Por exemplo, o URL da Procuradoria da República em São Paulo (www.prsp.mpf.gov.br) é identificada na rede pelo endereço IP 200.142.34.3, que é um número único em toda a rede mundial. A "tradução" dos nomes de

[1] No Brasil, o registro dos nomes de domínio é responsabilidade do Núcleo de Informação e Coordenação do Ponto BR - NIC.br, segundo a resolução n.º 001/2005 disponível em <http://www.cgi.br/regulamentacao/resolucao2005-01.htm>. Acesso em 01.03.2006

domínio para um endereço IP é feita por meio de um computador chamado servidor DNS (sigla de *Domain Name System – Sistema de Nomes de Domínios*).

Como é sabido, para que um usuário possa "navegar" nas páginas da Internet, e também receber e enviar e-mails, trocar arquivos de áudio ou vídeo, participar de grupos de discussão ou conversar com outras pessoas em *chats*, é preciso que esteja conectado à rede. A conexão é feita por intermédio de um **modem**, ligado a uma linha telefônica ou a um cabo. As concessionárias de telefone comercializam linhas especiais para a Internet, popularmente conhecidas como "banda larga", que utilizam sistemas ADSL (a*symetric digital subscriber* line) ou ISDN (*integrated services digital network*).

A conexão com a Internet depende ainda da assinatura de um **provedor de acesso** como UOL, Globo, IG, Terra, AOL, USP, Procuradoria da República. A regulação estatal da atividade desses provedores é mínima, o que dificulta as investigações criminais desenvolvidas no Brasil e, conseqüentemente, contribui para a impunidade de alguns crimes cibernéticos. Para reduzir o problema, as Procuradorias da República de alguns Estados vêm celebrando "termos de compromisso" (anexo III) com os provedores, pelos quais estes se obrigam a preservar os dados dos usuários pelo prazo mínimo de seis meses e a informar a polícia e o Ministério Público, tão logo tomem conhecimento de algum crime cometido em suas páginas.

Quando o usuário faz a conexão à rede, recebe um número – o *Internet Protocol* (IP) já referido. Esse número, *durante o tempo de conexão*, pertence exclusivamente ao usuário, pois é graças a ele que o internauta pode ser "encontrado" na rede. **A identificação do IP é o primeiro e mais importante passo para a investigação de um crime cibernético, como veremos adiante**. Convém, desde logo, lembrar que o investigador deve ainda identificar a **hora exata da conexão e o fuso horário do sistema**, pois um número IP pertence ao usuário apenas durante o período em que ele está conectado; depois, o número é atribuído a outro internauta, aleatoriamente.

3. OS CRIMES CIBERNÉTICOS.

Muitas coisas podem ser feitas pela Internet. Podemos pagar contas, trocar mensagens, participar de salas de bate-papo, "baixar" arquivos de música, imagem ou texto, comprar produtos, solicitar serviços, acessar *sites* contendo informações sobre todos os assuntos do conhecimento humano. Em todas essas atividades há o risco de encontrar alguém que se aproveita da velocidade e da escala em que as trocas de informações ocorrem na rede para cometer crimes.

A "Convenção sobre a Cibercriminalidade", adotada pelo Conselho da Europa em 2001[2] (anexo V), e aberta à assinatura por todos os países do globo, obriga os Estados a tipificar as seguintes condutas:

1. Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
   a) acesso doloso e ilegal a um sistema de informática;
   b) interceptação ilegal de dados ou comunicações telemáticas;
   c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracker*);
   d) atentado à integridade de um sistema;
   e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados;

2. "Infrações informáticas":
   a) falsificação de dados;
   b) estelionatos eletrônicos (v.g., os *phishing scams*);

3. Infrações relativas ao conteúdo:
   a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
   b) racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e

[2] Disponível no site: http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm.

ameaça qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade)[3];

4. Atentado à propriedade intelectual e aos direitos que lhe são conexos.

No Brasil, o projeto de lei n.º 84/99, de autoria do deputado Luiz Piauhylino, buscou dar um tratamento mais sistemático aos crimes cibernéticos. Um substitutivo da proposta foi aprovado pela Câmara dos Deputados em novembro de 2003 e atualmente aguarda a manifestação do Senado. Nossa legislação, porém, não apresenta muitas lacunas em matéria de crimes cibernéticos, havendo, inclusive, tipos penais específicos relativos a essa modalidade de delitos:

a) No capítulo dos crimes contra a administração pública, o art. 313-A do Código Penal sanciona a conduta de "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";

b) O art. 313-B contém a hipótese de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente";

c) A divulgação, sem justa causa, de informações sigilosas ou reservadas contidas ou não nos sistemas de informações ou banco de dados da Administração Pública é sancionada pelo art. 153, § 1º-A;

d) Ao servidor que viola o sigilo funcional, permitindo ou facilitando, "mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública", ou que se utiliza, indevidamente, do acesso restrito, há a incidência das penas previstas no art. 325 do Código Penal;

e) A Lei 10.764, de 12 de novembro de 2003, modificou a redação do art. 241 do Estatuto da Criança e do Adolescente para explicitar a possibilidade do crime de

[3] A repressão aos crimes de racismo e xenofobia praticados por intermédio de um sistema de informática está prevista, na verdade, no Protocolo Adicional à "Convenção sobre a Cibercriminalidade", de 30 de janeiro de 2003 (disponível no site: http://conventions.coe.int/Treaty/FR/Treaties/Html/189.htm).

pornografia infanto-juvenil ser praticado pela rede mundial de computadores. Além disso, previu a responsabilidade criminal daquele que "assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas" ou "assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens de pedofilia" (cf. item seguinte);

f) Além dos tipos penais que fazem menção explícita à informática, há outros em relação aos quais é possível haver a subsunção de condutas ilícitas executadas por meio da internet: o *cracker*, por exemplo, pode estar incurso no crime de dano, descrito no art. 163 do Código Penal. A prática ou incitação do racismo é reprimida pelo art. 20, *caput* e § 2º, da Lei 7.716/89. O *phishing scam* subsume-se perfeitamente ao delito de estelionato.

3.1. Breves comentários aos crimes do art. 241 do ECA.

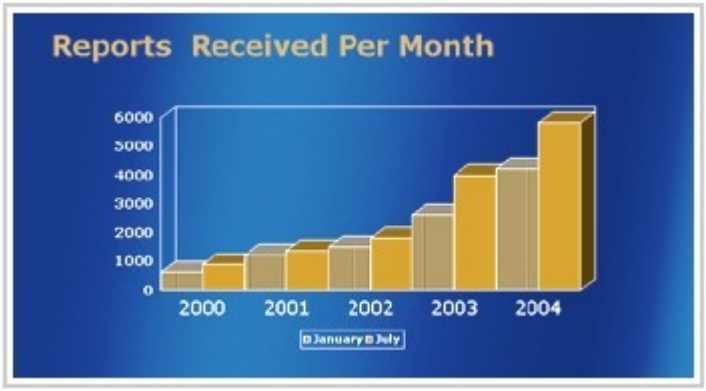
É sabido que o desenvolvimento das comunicações e da transmissão de dados à distância tem trazido incontáveis vantagens à humanidade. Os avanços tecnológicos ocorridos nos últimos anos tornaram a Internet uma ferramenta muito versátil e cada vez mais popular, de sorte que, num futuro não muito distante, computadores conectados à rede poderão substituir o papel e outros suportes de dados, como os CDs. Conseqüentemente, nossas vidas serão cada vez mais influenciadas pela tecnologia, revolucionando a percepção e a prática de atividades corriqueiras, tais como a leitura de um jornal, o envio de correspondências ou a audição de uma música.

Lamentavelmente, porém, as inovações da Internet vêm acompanhadas de todas as conseqüências do "mau uso" da tecnologia. O notável crescimento da rede mundial de computadores não criou muitas novas condutas antijurídicas, mas amplificou de forma extraordinária o dano causado pelas ofensas já conhecidas: um panfleto racista, no início do século passado, por exemplo, poderia ser lido, no máximo, por algumas centenas de pessoas; na Internet, porém, o mesmo conteúdo está disponível a mais de meio bilhão de pessoas e pode ser encontrado em poucos segundos.

O mesmo ocorre em relação à pornografia infantil. O relativo anonimato propiciado pela Internet favoreceu a produção e a distribuição de fotos e vídeos abjetos de crianças e adolescentes em cenas de sexo explícito. Possibilitou, também, que adultos assediem livremente crianças em salas de bate-papo virtuais, ou encontrem outros adultos portadores da mesma patologia em sites de pornografia ou comunidades de relacionamento.

O número de sites de pornografia infantil cresce a cada ano no mundo. Apenas no segundo semestre de 2004, mais de 5000 páginas de

pornografia foram denunciadas ao *hotline* mantido pela *Association of Sites Advocating Child Protection* (http://www.asacp.org).



Fonte: ASACP (www.asacp.org)

No Brasil, algumas organizações da sociedade civil recebem denúncias de pornografia infantil na Internet e as retransmitem para os órgãos envolvidos na persecução penal. A Procuradoria da República em São Paulo mantém convênio com os *hotlines* Safernet Brasil (www.safernet.org.br) e www.censura.com.br e temos obtidos bons resultados com essas parcerias.

A conduta de produzir ou distribuir fotografias ou imagens de pornografia infantil está tipificada no art. 241 do Estatuto da Criança e do Adolescente (Lei Federal 8.069/90), cuja redação original prescrevia:

> Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
>
> Pena: reclusão de 1 (um) a 4 (quatro) anos.

A despeito de inovador, tal preceito foi considerado tímido para a proteção do bem jurídico, razão pela qual foram apresentadas diversas propostas de alteração legislativa, com o objetivo de assegurar maior efetividade à repressão ao crime de pedofilia. O projeto de lei n.º 3.383/97, por exemplo, tipificava a disponibilidade de acesso de crianças e adolescentes a material com descrição ou ilustração de sexo explícito, pornografia ou violência em rede de computadores.

Apesar das infindáveis polêmicas sobre qual das propostas melhor adaptaria a lei penal à criminalidade cibernética de hoje, em especial ao crime de pornografia infantil praticado através da rede mundial de computadores, optou-se por modificar o já existente tipo penal do art. 241, da Lei nº 8.069/90. Isso foi feito pela Lei Federal nº 10.764, de 12 de novembro de 2003, que conferiu ao artigo a seguinte redação:

> Art. 241. *Apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.*
>
> *Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa.*
>
> *§ 1º Incorre na mesma pena quem:*
>
> *I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;*
>
> *II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;*
>
> *III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do* caput *deste artigo.*
>
> *§ 2º A pena é de reclusão de 3 (três) a 8 (oito) anos:*
>
> *I – se o agente comete o crime prevalecendo-se do exercício de cargo ou função;*
>
> *II – se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.*"

Com a alteração legislativa, como se vê, o art. 241 do ECA passou a prever expressamente o crime de divulgação e publicação, pela Internet, de imagens e fotografias de crianças e adolescentes em cenas de sexo explícito.

É relevante indagar, nesse passo, se o tipo penal abrange também a divulgação de desenhos hiper-realistas de crianças em situação sexual, ou se a proteção criminal abrange tão somente a transmissão ou publicação de filmes ou fotografias envolvendo crianças "reais". Nos debates parlamentares houve a rejeição de emenda apresentada pelo Deputado Antonio Carlos Biscaia (PT-RJ), que previa a repressão a *"qualquer representação, por qualquer meio, de criança ou adolescente no desempenho de atividades sexuais explícitas ou simuladas."*

Por outro lado, a cabeça do artigo refere-se não apenas a fotografias, mas também a "imagens". Assim, pensamos que desenhos, montagens e composições que retratem crianças em cena de sexo explícito podem, em tese, configurar o crime.

É importante mencionar, ainda, que o art. 241, § 1º, do ECA tornou possível a responsabilização criminal dos administradores de provedores de acesso e de hospedagem de páginas, quando estes, dolosamente, *assegurem os meios ou serviços para o acesso ou armazenamento* na rede das fotografias, cenas ou imagens produzidas na forma do caput do artigo. O crime não admite forma culposa, de modo que é preciso comprovar que o responsável pelo provedor tinha ciência da existência de material com tais características em seu sistema informático. A

observação é importante porque há provedores de hospedagem gratuita – como o hpG, mantido pelo IG – que armazenam milhares de páginas, não sendo razoável supor que os responsáveis pelo serviço tenham, *a priori*, conhecimento de eventuais páginas criminosas mantidas no provedor. Todavia, uma vez cientes da existência da página, os responsáveis pelo provedor têm o dever de informar a polícia ou o Ministério Público sobre o fato, pena de responderem pelo delito tipificado no art. 241, § 1º, incisos II ou III, do Estatuto da Criança e do Adolescente.

Não temos, até o momento, conhecimento de acórdãos que versem sobre as modificações introduzidas pela Lei Federal nº 10.764/03. O Supremo Tribunal Federal, em dois julgados, entendeu que qualquer instrumento hábil a tornar público o material proibido está incluído na compreensão do verbo "publicar", inclusive a Internet (cf. a jurisprudência compilada no anexo I deste manual).

A objetividade jurídica do tipo é a integridade física, a liberdade sexual, a dignidade e a honra da criança ou adolescente. Entendemos que o crime é de perigo, havendo, portanto, a incidência do delito, ainda quando não se saiba a identidade da criança ou do jovem retratado.

Sujeito ativo do crime tipificado no *caput* do artigo é qualquer pessoa. As condutas descritas nos incisos II e III do § 1º, e no inciso I do § 2º, por sua vez, são delitos próprios, na medida em que só podem ser praticados por determinadas pessoas (aqueles que asseguraram o armazenamento das fotografias ou imagens na Internet e o acesso do criminoso à rede).

Em muitos casos, quando a vítima é púbere, não é possível dizer, com a certeza exigida para o ajuizamento da denúncia, que houve a divulgação de imagem de menor de 18 anos. Nesses casos, temos optado por arquivar o procedimento, sem prejuízo do disposto no art. 18 do Código de Processo Penal.

O momento da consumação do crime enseja, certamente, muitas dúvidas na doutrina. Entendemos que se o agente mantiver a fotografia ou imagem em uma determinada página eletrônica, o crime será *permanente*. Em contrapartida, se o criminoso remeter a fotografia ou imagem para um destinatário específico, o crime será instantâneo.

4. A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS.

Quando recebemos a notícia de um crime cibernético, a primeira providência a tomar é a **identificação do meio usado**: trata-se de a) um *website?*; b) um e-mail?; c) programas de troca de arquivos eletrônicos (do tipo *Kazaa*)?; d) arquivos ou mensagens ofensivas trocados em programas de mensagem instantânea (do tipo *MSN Messenger* ou *ICQ*)?; e) arquivos ou mensagens ofensivas trocados em salas de bate-papo (*chats*)?; f) grupos de discussão (como *yahoo groups*)?; ou g) comunidades virtuais como o *Orkut*? As características de cada um desses meios são diferentes e, por isso, as medidas a serem tomadas são igualmente distintas.

De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características:

a) possuem formato complexo (arquivos, fotos, dados digitalizados etc.);

b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente;

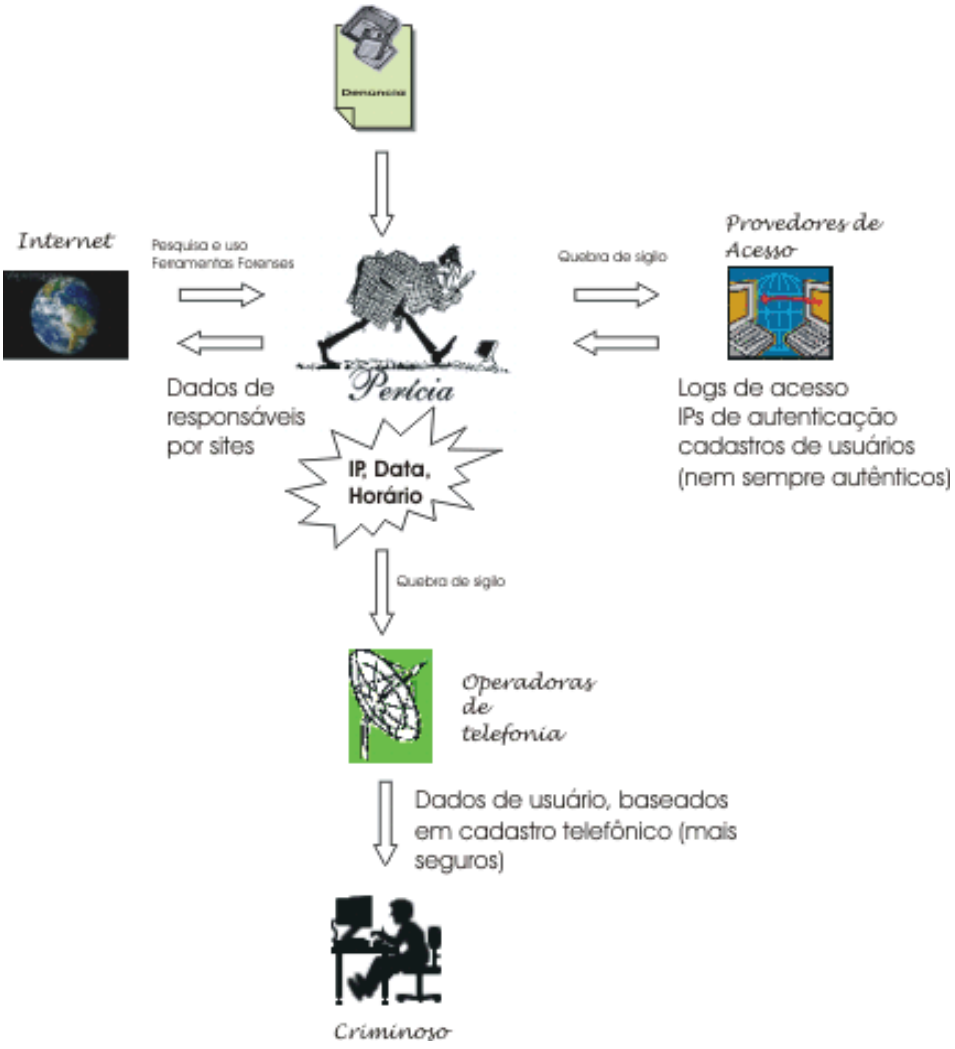
c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Como já dito, uma das mais importantes evidências que podemos coletar é o chamado **número IP** (*Internet Protocol*). O número IP é uma identificação que todos os computadores que acessam a Internet possuem; ele aparece no formato A.B.C.D, onde A, B, C e D são números que variam de 0 a 255 (por exemplo, 200.158.4.65). O IP deve estar acompanhado da data, hora exata da conexão ou comunicação e o fuso horário do sistema. Por exemplo:

Received: from mailserver.uol.com.br ([**200.143.23.48**]) by mc1-f23.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); **TUE, 1 FEB 2005 05:41:12 (-0800)**

Como a Internet é uma rede *mundial* de computadores, os registros indicam a hora local (05:41:12, no exemplo) e a referência à hora GMT (no caso -08:00). Às vezes, é feita apenas a menção à hora GMT (por exemplo, “Tue, 09 Mar 2004 00:24:28 GMT”). **Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.**

A ilustração abaixo busca representar o caminho básico percorrido pela investigação de um crime cibernético:



Observação importante: antes de tomar qualquer providência a respeito de uma notícia recebida, recomendamos vivamente que o investigador providencie a proteção de seu computador contra ataques digitais. Há, hoje, mais de 100 mil vírus catalogados pelas empresas de segurança. E não são apenas eles que provocam danos e comprometem a segurança do computador. Há ainda "pragas" como *worms*, *spywares* e "cavalos de Tróia".

"*Cavalos de Tróia*" ou *trojans* - à semelhança da invenção mitológica - são programas aparentemente inofensivos que contêm códigos maliciosos capazes de destruir dados armazenados, enviar informações sigilosas e até mesmo permitir que o *cracker* tenha acesso ao computador.

Vírus são *malwares (softwares* maliciosos) criados com o objetivo de danificar arquivos armazenados no disco rígido (especialmente arquivos críticos para o funcionamento do sistema), tornando o sistema inoperante. *Worms* são como os vírus, mas têm a capacidade de se propagar para outros computadores. Normalmente, os *worms* geram um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede. Os *worms* constumam se propagar buscando vulnerabilidades em sistemas e em e-mails. Para evitar que seu computador seja danificado, é muito importante manter os programas de proteção permanentemente atualizados e nunca abrir e-mails enviados por remetentes estranhos, sobretudo se estiverem acompanhados de arquivos com extensão ".exe", ".src", ".bat" e ".pif".

Spywares são programas espiões, usados geralmente com fins comerciais. São instalados quando o usuário recebe algum e-mail, baixa algum arquivo ou navega pela Internet. Uma vez executados, passam a monitorar as páginas acessadas e o que é digitado pelo usuário. As conseqüências de um programa-espião incluem a lentidão no acesso à Internet, a mudança da página inicial do *browser* e a proliferação daquelas pequenas janelas, conhecidas como "*pop-ups*".

Nos últimos anos têm ocorrido a proliferação de redes de computadores infectados, conhecidos como *botnets.* Essas redes são criadas para furtar dados, enviar *spams* em larga quantidade, trocar programas piratas e, principalmente, obter vantagens financeiras. Tudo começa com o recebimento de um e-mail falso, supostamente remetido por uma instituição conhecida, como um banco ou órgão governamental (TRE, Receita Federal, Polícia Federal...). Os e-mails contêm arquivos maliciosos anexados ou acessados quando o usuário seleciona um determinado link inserido no texto da correspondência. Aberto o arquivo, um robô (*bot*) é instalado no computador do usuário. Através da Internet, o robô conecta o computador a uma rede (*botnets*) controlada por um *cracker.* Este ciber-criminoso pode remotamente controlar as máquinas dos usuários vinculados à rede, obtendo dados como senhas e números de cartões e furtando arquivos pessoais e dados internos do sistema. Essas redes vem evoluindo de forma tão intensa que as operações são realizadas automaticamente, sem a necessidade de intervenção do *cracker*.

As vantagens financeiras obtidas pelo *cracker* incluem:

- venda dos dados de cartão de crédito;
- aluguel de *botnets* para a realização de ataques DDoS (*Distributed Denial of Service*). Trata-se do envio de muitas requisições simultâneas a um determinado serviço, com o objetivo de torná-lo inoperante. Há registros de *botnets* contendo mais de um milhão e meio de máquinas. Se apenas 10% das máquinas dessa rede, enviarem uma requisição a um serviço ao mesmo tempo, o sistema certamente entrará em colapso;

- venda de *proxys* abertos, para facilitar a comunicação entre criminosos e o envio de spam;
- venda de seriais de programas proprietários;
- roubo de dados pessoais, para pedir posterior resgate a vítima;
- realização de subtração de valores de contas bancárias de suas vítimas.

A proliferação desses robôs é causada pela sua capacidade de buscar novas máquinas para infectar. Ou seja, basta que apenas um computador seja infectado para que os outros computadores da rede fiquem potencialmente vulneráveis.

No site www.download.com é possível encontrar antivírus, anti-*spywares* (*Ad-Aware* e *Spybot* são dois deles), *firewalls* (veja Zone Alarm ou OutPost) e outros programas que aumentam a segurança do computador. Muitos desses programas são gratuitos. **Recomendamos que: a) o usuário faça periodicamente a atualização dos programas de seu computador (especialmente do *Windows*); b) instale, em seu micro, um *firewall* (programa que dificulta a invasão de cr*ackers*) e filtros *anti-spam*; c) evite abrir e-mails desconhecidos, especialmente quando façam referência a *links* ou tragam anexados programas ou arquivos; d) crie um e-mail específico para trabalhar com investigações, de preferência vinculado a um provedor estrangeiro (*G-Mail*, *Hotmail, Yahoo* etc.); e) utilize, preferencialmente, uma máquina exclusiva para investigação, evitando o uso de computadores com dados pessoais e de trabalho.**

O site http://www.virustotal.com/flash/index_en.html disponibiliza um serviço pelo qual é possível submeter um arquivo suspeito à avaliação.

Apresentamos, em seguida, os principais meios eletrônicos sobre os quais podem recair a investigação criminal, e as providências iniciais necessárias à coleta da prova:

4.1. WEBSITES:

4.1.1. Evidências necessárias:

Não é suficiente o endereço URL (exemplo: www.usp.br) para iniciar uma investigação, pois, como dissemos, as evidências nos crimes eletrônicos são voláteis, i.e., podem ser apagadas, alteradas ou perdidas

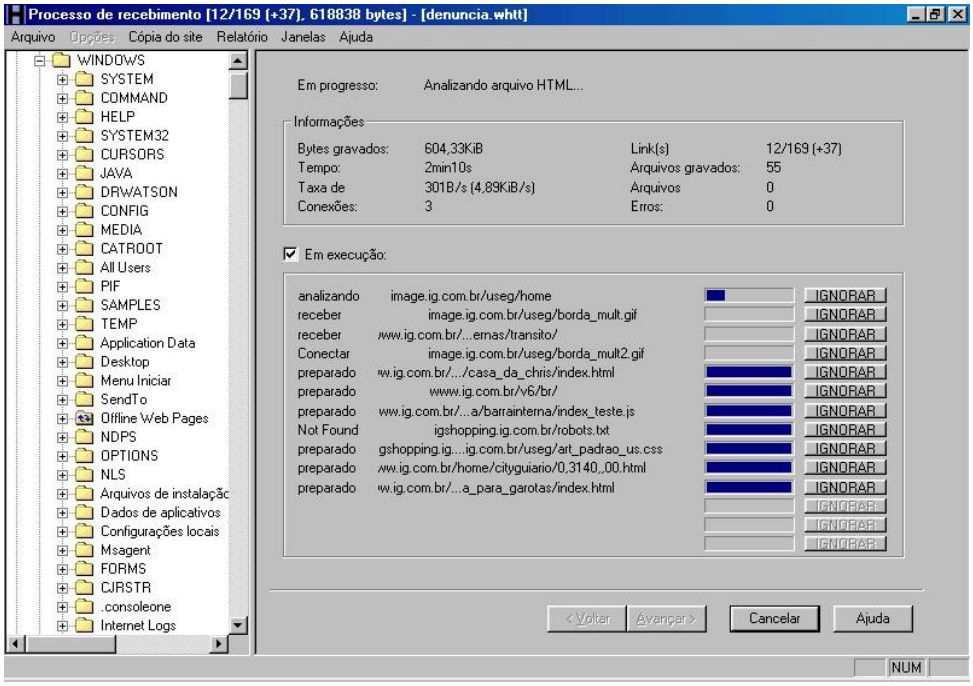
facilmente. Assim, se a *notitia criminis* não estiver acompanhada da página impressa, é preciso, antes de mais nada, providenciar a impressão do *site* ou, melhor ainda, o *download* de seu conteúdo (ver item seguinte).

4.1.2. **Salvando o conteúdo inteiro do *site.***

Existem aplicativos – por exemplo, o *HTTrack*[4] - que permitem o *download* de *sites* inteiros, incluindo textos e fotos publicadas. Utilizar estes aplicativos é um artifício interessante para casos onde o volume de dados é grande.

Após o *download*, os arquivos podem ser encaminhados para o órgão competente através de e-mails, disquetes e, se possível, em mídia não-regravável (CD-R).

Abaixo apresentamos uma tela do software *HTTrack* fazendo o *download* de um site:



O HTTrack, além de permitir o *download* parcial ou total do *site*, também gera um arquivo de *log* (hts_log) registrando a data, hora e endereço do *site* salvo. Essas informações servirão para definir o tempo do crime.

Para sistemas Unix e assemelhados (ex: GNU/Linux), o utilitário apropriado para se copiar o conteúdo de um site é o software livre *wget*[5]. Assim como o HTTrack, esse programa também gera um arquivo de *log*,

[4] Gratuitamente disponível no site http://www.httrack.com
[5] Página do wget: http://www.gnu.org/software/wget/

além de permitir diversas configurações que auxiliam na investigação. Um exemplo de *download* dos arquivos *.jpg*[6] de um site com o wget:

```
investigador@mpf-sp:~$ wget -r -A.jpg http://www.prsp.mpf.gov.br/
--06:13:32--  http://www.prsp.mpf.gov.br/
          => `www.prsp.mpf.gov.br/index.html'
Resolvendo www.prsp.mpf.gov.br... 200.142.58.20
Connecting to www.prsp.mpf.gov.br|200.142.58.20|:80... conectado!
HTTP requisição enviada, aguardando resposta... 200 OK
Tamanho: 22,171 (22K) [text/html]
100%[==============================================>]                 22,171
60.93K/s
06:13:53 (60.83 KB/s) - `www.prsp.mpf.gov.br/index.html' saved [22171/22171]
```

Um front-end (interface gráfica) para o wget é o programa *gwget:*

4.1.3. Salvando e garantindo a integridade dos dados (procedimento ideal):

No curso do processo penal, a autenticidade das evidências colhidas pode ser impugnada pela defesa. Para evitar esse tipo de problema, nos casos onde não é possível gravar os arquivos em mídia não-regravável, é importante a utilização de um aplicativo que garanta a integridade dos dados. O MD5Sum[7] é um aplicativo de verificação da integridade dos dados;

[6] JPG é um formato de compressão de imagem muito comum na *Web* e bastante utilizado na distribuição de pornografia infantil.

[7] Pode ser baixado gratuitamente no site: www.md5summer.org.

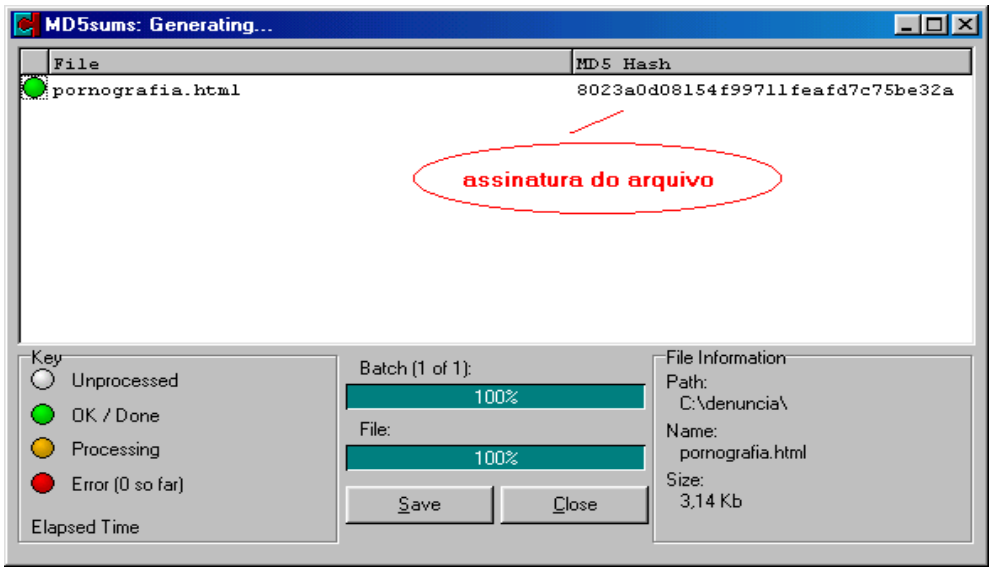
na prática ele garante que os dados que foram gravados no momento da produção da prova não sofreram nenhum tipo de adulteração em todo o trâmite do processo.

Tecnicamente, ao criarmos uma cópia de algum arquivo, criamos também sua assinatura baseada no arquivo original. Esta assinatura, em forma de um arquivo, acompanhará a cópia e permitirá que a qualquer momento o destinatário verifique se o arquivo recebido é idêntico ao original.

Como utilizar o *MD5Sum*?

1. Compacte seus arquivos para gerar somente um arquivo .ZIP (é mais fácil gerar a assinatura de um só arquivo do que de todos);
2. Rode o programa MD5Sum para esta cópia gerada;
3. Mande a cópia de seu arquivo zipado, junto com este arquivo adicional criado (assinatura) com extensão .MD5.
4. Com este arquivo (assinatura) o receptor de seu arquivo poderá a qualquer momento rodar o MD5Sum no arquivo recebido e comparar as assinaturas, se forem iguais, o arquivo é autêntico.

Abaixo uma tela do MD5Sum criando uma assinatura de um arquivo:



4.1.4. Outras softwares que auxiliam a investigação.

Além dos utilitários que auxiliam na cópia parcial ou integral do *site* investigado existem outras ferramentas capazes de facilitar o trabalho do investigador. Navegadores em modo texto, a exemplo do LYNX[8], facilitam a identificação de *links* internos e externos do site investigado. Para identificarmos todos os links contidos na página inicial da Procuradoria da República em São Paulo, utilizamos o comando:

```
lynx --dump www.prsp.mpf.gov.br
```

que retorna o seguinte resultado:

```
  1. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#banner
  2. http://www.prsp.mpf.gov.br/
  3. http://www.prsp.mpf.gov.br/acessibilidade/acessibilidade.htm
  4. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#Map
  5. http://www.prsp.mpf.gov.br/digidenuncia.htm
  6. http://www.prsp.mpf.gov.br/atuacao/atuacao.htm
  7. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#licitacao
  8. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#contas
  9. http://producao.prsp.mpf.gov.br/news/internews/news_noticias.php
 10. http://www.prsp.mpf.gov.br/noticiasindice.htm
 11. http://www.prsp.mpf.gov.br/prdc/
 12. http://www2.pgr.mpf.gov.br/concurso/concurso-de-procuradores/index_html
 13. http://www.pgr.mpf.gov.br/pgr/concursos/servidor/index.htm
 14. http://www.prsp.mpf.gov.br/outroslinks/concursos/estagiario.htm
 15. http://www.prsp.mpf.gov.br/outroslinks/informes/clipping.htm
 16. http://www.prsp.mpf.gov.br/outroslinks/informes/notdefic.htm
 17. http://www.prsp.mpf.gov.br/outroslinks/informes/informes.htm
 18. http://www.prsp.mpf.gov.br/abnt/abnt.htm
 19. http://producao.prsp.mpf.gov.br/plantao/plantaocapital.pdf
 20. http://producao.prsp.mpf.gov.br/plantao/plantaointerior.pdf
 21. http://producao.prsp.mpf.gov.br/plantao/plantaojuizes.pdf
 22. http://producao.prsp.mpf.gov.br//consultaprocessual/consproc_consulta_rapida.php
 23. http://www.prsp.mpf.gov.br/acessibilidade/acessibilidade.htm
 24. http://www.prsp.mpf.gov.br/
 25. http://www.prsp.mpf.gov.br/repensando.pdf
 26. http://www.prsp.mpf.gov.br/Templates/procuradoria/organograma/prdc.htm
 27. http://www.prsp.mpf.gov.br/audp/audp.htm
 28. http://www.prsp.mpf.gov.br/credenc.htm
 29. http://www.prsp.mpf.gov.br/procuradoria/municipios.htm
```

Outra ferramenta bastante útil é um acessório do navegador Mozilla-Firefox, disponível gratuitamente no endereço https://addons.mozilla.org/extensions/moreinfo.php?id=590&application=firefox. A extensão mostra, na barra de *status* do navegador, o número IP do *site* visitado, e fornece ainda uma série de ferramentas para tratar a informação.

[8] http://lynx.browser.org/

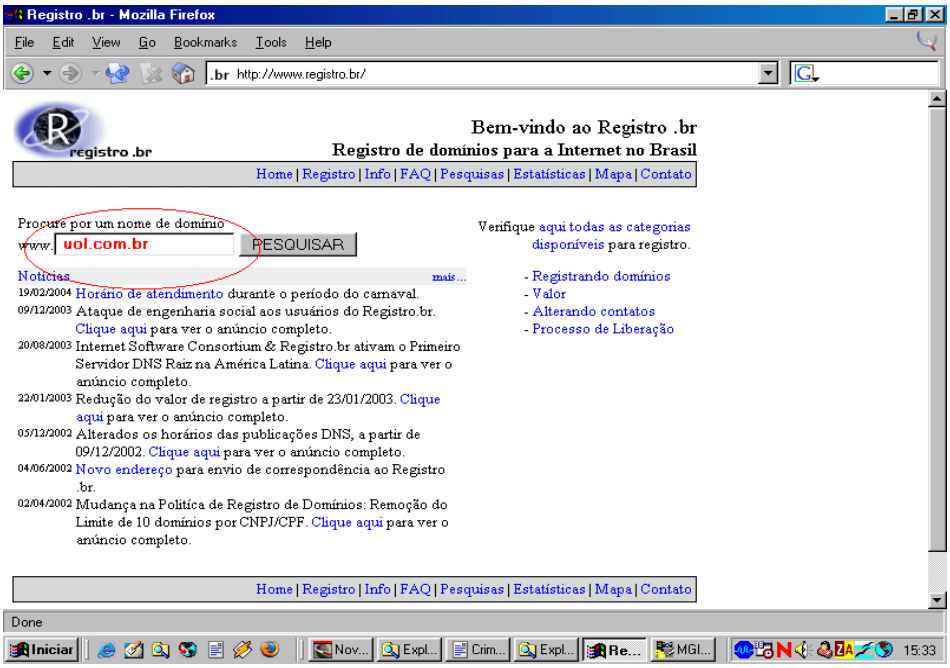
Com apenas um clique é possível obter informações importantes, como o país onde a página está sediada e a empresa responsável por sua hospedagem.

4.1.5. **Pesquisa de domínios (localizando o responsável por um *site*).**

Depois de preservar a prova, o passo seguinte é a identificação do servidor que hospeda a página. Há ferramentas de busca na Internet que fazem esse serviço. É preciso apenas verificar se o *site* é nacional (ou seja, se as letras finais do nome do domínio são “br") ou estrangeiro.

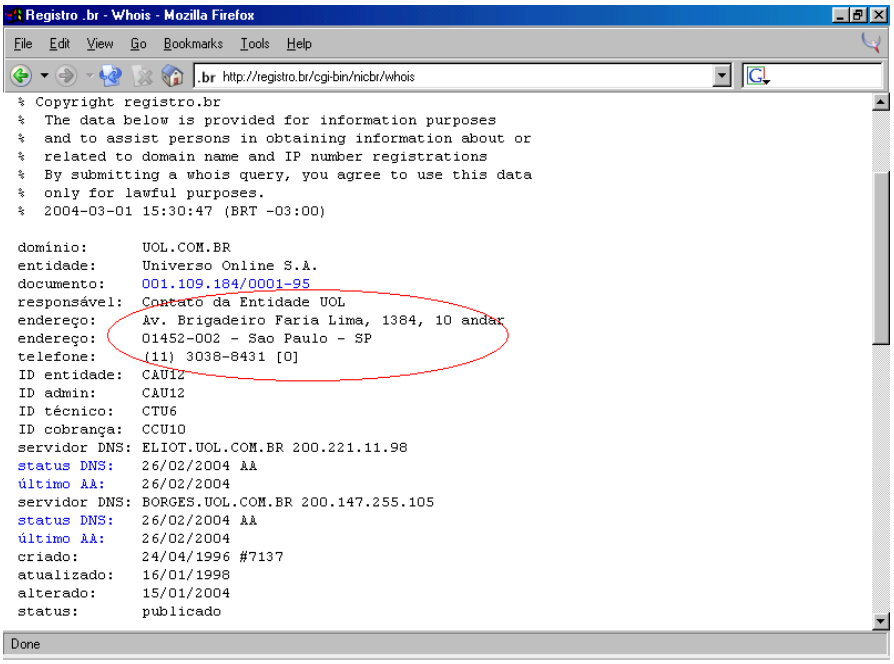
4.1.5.1. Domínios nacionais (“.br”).

Os sites que ficam sobre a administração do NIC.br são facilmente identificados pela terminação “.br” e podem ser pesquisados pelo site do http://www.registro.br



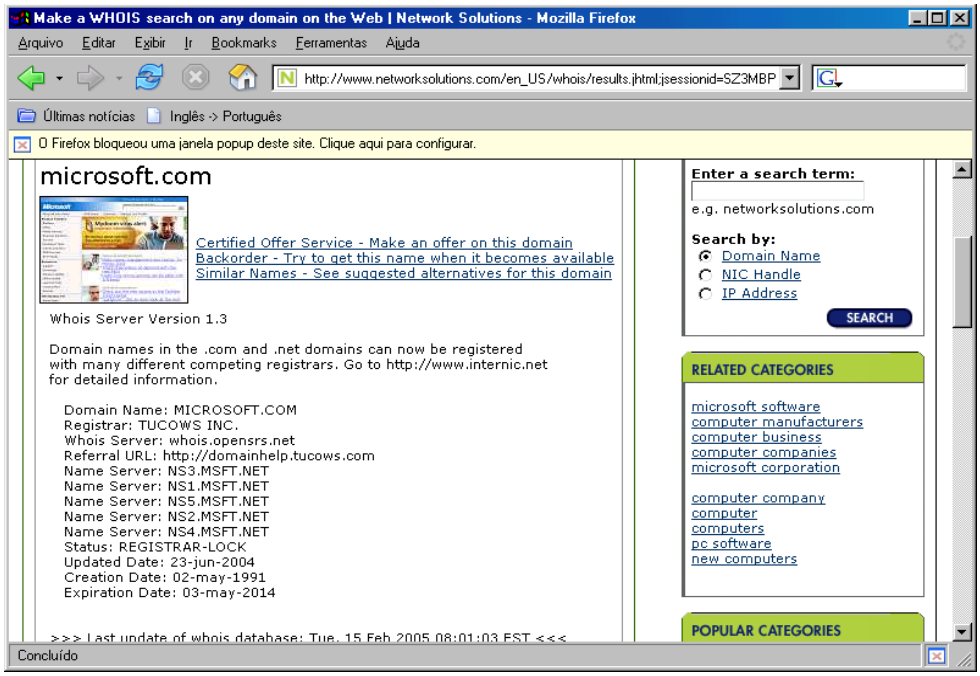
O resultado desta pesquisa pode trazer informações importantes como o nome do responsável administrativo pelo domínio, o contato de incidentes de segurança (responsável pelo Setor de Tecnologia de Informação) e o provedor de *backbone* (empresa que detêm blocos de endereços IPs).

Abaixo uma tela contendo o resultado de pesquisa de um *site*:



4.1.5.2. Domínios estrangeiros.

A pesquisa de sites estrangeiros pode ser feita por diversos serviços de WHOIS, dentre eles http://www.arin.net/; http://www.internic.net/whois.html; http://lacnic.net/ e http://www.netoworksolutions.com. Outro serviço muito bom para investigações de sites estrangeiros leva o nome do cínico detetive de Dashiell Hammett: http://www.samspade.org. Veja abaixo um resultado de busca no WHOIS:



Caso o site esteja hospedado no exterior, a competência da Justiça e da Polícia brasileiras só estará justificada (e executável) se houver algum vínculo com brasileiros. Por exemplo, há hoje *sites* racistas e nazistas feitos por brasileiros hospedados em provedores na Argentina e nos EUA. Nesse caso, entendemos que é possível a persecução penal no Brasil, remanescendo o problema da identificação da autoria.

Se não houver vínculo algum do *site* com o Brasil (ou seja, ele não está hospedado em provedores nacionais e não há indícios da participação de brasileiros no delito) recomendamos que a notícia do fato criminoso seja encaminhada à INTERPOL. Ou, melhor, comunicada a um dos *hotlines* associados à INHOPE - International Association of Internet Hotlines (www.inhope.org), pois a associação filiada se encarregará de informar rapidamente a polícia local.

Dica:

Alguns *sites*, mesmo hospedados em provedores externos, trazem *links* do tipo “contato” ou “webmaster”, com a indicação de um endereço de e-mail.

Vale a pena pesquisar este e-mail, pois às vezes ele pode indicar algum responsável pelo conteúdo do *site*.

4.1.6. Quebra do sigilo de dados telemáticos.

Feita a identificação do provedor que hospeda a página, qual a etapa seguinte? Depende: a) se o hospedeiro é um provedor conhecido, que hospeda, gratuita ou mediante remuneração, *sites* de terceiros (por exemplo, “HPG”, “Geocities”, “Terra”); b) se a página está registrada em nome de uma empresa não conhecida. Nessa última hipótese, seria preciso analisar o caso concreto, e verificar se é possível requerer a quebra do sigilo de dados telemáticos sem que o autor da página tome conhecimento disso.

Se o provedor que hospeda a página for conhecido (e brasileiro), o investigador deverá requerer, judicialmente (ver modelo no anexo III), a quebra de sigilo de dados telemáticos, para que o hospedeiro forneça uma cópia, em mídia não-regravável (CD-R), das páginas investigadas e também os *logs*, isto é, os registros de criação e alteração da página. É no *log* que encontramos as três informações que nos são necessárias para prosseguir: a) o número IP; b) a data e a hora da comunicação; e c) a referência ao horário, incluído o fuso horário GMT ou UTC.

No caso de páginas da Internet, é comum o provedor fornecer uma lista de IP’s e datas. Esta lista indica todas as vezes em que a página foi modificada. Como é possível que mais de um computador tenha sido usado para alterar o conteúdo da página, aconselhamos que o investigador selecione quatro ou cinco “linhas” da lista para, em seguida, formular outro requerimento judicial, desta vez à operadora de telefonia ou cabo.

4.1.7. Localizando o "dono" de um IP.

Como dissemos, o número IP é uma identificação que todos os computadores que acessam a Internet possuem. Essa identificação pode ser estática (i.e., pertence a uma pessoa determinada, por um certo período de tempo) ou dinâmica (aleatoriamente atribuídas a um usuário). Organizações como empresas e universidades normalmente possuem uma faixa de IP's próprios, e a identificação do usuário depende da política interna de conexão da instituição.

Para usuários domésticos, o mais comum é o IP dinâmico, fornecido por uma operadora de comunicação, normalmente, provedores de acesso (UOL, Globo, IG etc.). As informações de quem usava o endereço IP em um determinado dia e horário devem ser buscadas nas operadoras de comunicação.

Como, então, saber a qual instituição pedir as informações? É simples: basta repetir as pesquisas mencionadas no item 4.1.5. Por exemplo: a qual empresa pertence o IP 200.153.238.195? Os números IP iniciados com "200" pertencem, geralmente, a concessionárias brasileiras. Digitando o número 200.153.238.195 no *site* www.registro.br[9] (no campo "procure um nome de domínio") descobrimos que o usuário conectou-se à Internet por meio de uma linha fornecida pela Telecomunicações de São Paulo S.A. – TELESP. O próprio *site* já fornece o nome do responsável e o endereço para onde o ofício judicial deverá ser encaminhado.

Localizado o provedor de acesso, que pode ser um provedor de Internet, uma organização particular ou uma companhia telefônica, a autoridade policial ou o Ministério Público deverá requerer ao juiz (ver modelo no anexo III) **novo pedido de quebra do sigilo de dados telemáticos**, desta vez para que o provedor de acesso informe as informações do usuário vinculado ao IP, em uma determinada data e horário. A concessionária deverá responder à ordem judicial fornecendo as informações necessárias para a identificação do indivíduo usuário do IP no momento solicitado, inclusive o endereço físico.

De posse dessas informações, o investigador poderá, se entender cabível, requerer a expedição de um mandado judicial, para a busca e apreensão do computador, de disquetes e de outros materiais.

---

[9] Outro *site* que possui diversas ferramentas para a localização de responsáveis por um IP está localizado no endereço http://www.network-tools.com.

Cyber-Cafés, Lan-Houses, Wireless...

É muito comum encontrar *cyber-cafés* e *lan-houses* instalados nas cidades brasileiras. A maioria não mantêm nenhum registro de usuários, o que praticamente impede a investigação de eventuais crimes por eles cometidos, já que não é possível identificá-los. Em algumas cidades e Estados há leis que obrigam esses estabelecimentos a manter um cadastro de seus usuários; é preciso admitir, porém, que o grau de eficácia dessas normas é muito pequeno.

Outro problema sério que deverá ser enfrentado nos próximos anos é o uso crescente de sistemas de transmissão sem fio (*Wireless* ou *Wi-Fi*). A tecnologia permite a conexão entre equipamentos de forma simples e fácil, pois os dados são transmitidos através de ondas eletromagnéticas. A maioria dos *notebooks* comercializados nos últimos meses já vem com a facilidade. Apesar das muitas vantagens do sistema (mobilidade, flexibilidade, custo reduzido, instalação simples...), há duas desvantagens que facilitam a prática de crimes: a) a vulnerabilidade a acessos não autorizados; e b) a dificuldade de identificação do computador que acessou a rede, através desse sistema: com efeito, qualquer pessoa que estiver na área de abrangência das ondas emitidas pelo ponto de acesso poderá praticar, anonimamente, toda a sorte de delitos. Considerando que as redes sem fio já estão funcionando em aeroportos, faculdades e cafés nas grandes cidades brasileiras, será preciso encontrar rapidamente formas de tornar o sistema mais seguro.

Mais uma vez lembramos que nos requerimentos endereçados aos provedores e concessionárias de acesso deve haver referência expressa: a) ao número IP; b) à data e a hora da comunicação; e c) ao horário GMT.

4.2. E-MAILS.

4.2.1. Evidências necessárias.

Quando a evidência investigada for um *e-mail* (por exemplo, uma mensagem que contenha arquivos com pornografia infantil anexados) é preciso não apenas preservar o conteúdo da mensagem, como também **identificar o cabeçalho do *e-mail*,** ou seja, a parte do e-mail que informa os dados do remetente e do destinatário da mensagem. O objetivo é aquele já mencionado: descobrir o número do IP, a data e a hora da transmissão e a referência à hora GMT.

Com a disseminação de vírus que alteram o remetente e com a falha de diversos aplicativos de *e-mails*, os quais permitem o preenchimento do campo “de” (remetente) sem autenticação, nem sempre o endereço que

consta no campo remetente, realmente mostra o verdadeiro autor da mensagem. Daí a importância do cabeçalho do *e-mail* numa denúncia que envolva algum tipo correio eletrônico.

4.2.2. **Localizando o cabeçalho do *e-mail*.**

Em aplicativos como o *Outlook* ou *Outlook Express*, o cabeçalho de um *e-mail* pode ser acessado abrindo a mensagem e clicando *Alt* + *Enter*. Outra opção é clicar, com o botão direito do *mouse*, em cima da mensagem recebida e selecionar "Opções". Na parte de baixo da janela aberta, há uma série de informações, agrupadas no título "Cabeçalho de Internet".

No *groupwise* (aplicativo utilizado no Ministério Público Federal), podemos localizar o cabeçalho de um *e-mail* abrindo a mensagem e clicando no Menu Arquivo – Anexos – Ver . Selecione o arquivo MIME.822.

Nos acessos feitos via Internet – como nos sistemas WEBMAIL e WEBACESS – os provedores costumam trazer opções no MENU que permitem editar e imprimir cabeçalhos de e-mails. Algumas dessas opções aparecem com o título "ver código fonte da mensagem" ou "verificar código completo", ou ainda "mensagem em formato texto". Caso não existam estas opções, basta encaminhar o e-mail para uma outra conta, e usar o Outlook para editar o cabeçalho de e-mail.

4.2.3. Analisando o cabeçalho de um e-mail.

A análise do cabeçalho de um *e-mail* é bastante complexa, mas é graças a ela que é possível identificar o remetente da mensagem.

É comum um cabeçalho possuir várias linhas que começam com a palavra "*received*". A palavra marca por quantas estações (ou servidores) a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o **último "*received*"**[10]; é ele quem indica a primeira máquina que originou a mensagem, isto é, o computador do remetente..

Abaixo um exemplo de cabeçalho de e-mail com endereço falso (típico de estação infectada com vírus), mas contendo o IP verdadeiro do remetente. Observe também a data e o horário (incluindo o fuso horário) que o e-mail foi encaminhado:

[10] Os "*received"* estão em ordem decrescente, ou seja, o primeiro "*received"* mostrará a máquina mais recente por onde sua mensagem passou.

```
Received: from pppp.mmm.gov.br
        ([200.158.14.238])
        by pppr.mmm.mmm.gov.br; Wed, 03 Mar 2004 07:49:53 -0300
From: pjfkdjkgab@jfpp.gov.br
To: fulano@pppp.mmm.gov.br
Subject: Re: Your archive
Date: Wed, 3 Mar 2004 07:46:27 -0300
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0003_000052ED.00002596"
X-Priority: 3
X-MSMail-Priority: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_0003_000052ED.00002596
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: 7bit
```

Um outro exemplo de cabeçalho de *e-mail*, que mostra o endereço eletrônico, a data e o horário (apenas GMT):

```
Received: from mpp.gov.br
        (rubi.mpp.gov.br [200.148.51.26])
        by ppppp.pppr.mpp.gov.br; Mon, 08 Mar 2004 21:17:35
-0300
Received: (qmail 3295 invoked by uid 306); 9 Mar 2004
00:15:46 -0000
Received: from direto@mkt.navio.com.br by rubi by uid 303 with
qmail-scanner-1.20
 ( Clear:RC:0(200.184.163.136):.
 Processed in 0.035505 secs); 09 Mar 2004 00:15:46 -0000
Received: from unknown (HELO mkt3.site.br.navio)
(200.184.163.136)
  by rubi.mpp.gov.br with SMTP; 9 Mar 2004 00:15:46 -0000
Received: from mkt3 ([172.26.0.243]) by mkt3.site.br.navio with
Microsoft SMTPSVC(5.0.2195.6713);
         Mon, 8 Mar 2004 21:24:29 -0300
From:    navio Direto <direto@mkt.navio.com.br>
To:      maria <maria@pppr.mpp.gov.br>
Date: Tue, 09 Mar 2004 00:24:28 GMT
Organization: navio
X-MSMail-Priority: Normal
X-mailer: AspMail 4.0.4.03 (SMT4D9FD2F)
```

`

4.2.4. Localizando o "dono" de um e-mail:

O número IP encontrado deve pertencer a uma operadora de telefonia. Para saber a qual concessionária pertence o número, o investigador deverá executar o procedimento descrito no item 4.1.7. deste manual. Se o número IP pertencer a um provedor de acesso, a providência necessária é aquela do item 4.1.6.

Se não foi possível localizar o número IP que originou a mensagem, mas há o endereço eletrônico do remetente (exemplo: joaodasilva@terra.com.br), a autoridade policial ou o membro do Ministério Público podem requerer judicialmente a quebra do sigilo de dados telemáticos para que o provedor do e-mail (no exemplo, o Terra) forneça o número IP da máquina que autenticou esta conta, na data e horário do e-mail remetido (ver modelo anexo). Caso queiram uma abrangência maior, poderão pedir a relação de todos os IPs gerados no momento de autenticação da conta, num determinado período (um mês, por exemplo).

Se o provedor do e-mail não estiver sediado no Brasil (exemplos: xxxxxxxx@*hotmail.com* ou xxxxxxxx@*yahoo.com*), o investigador encontrará dificuldades para obter as informações necessárias ao prosseguimento das investigações. O provedor de *e-mails Hotmail*, um dos mais populares do mundo, é mantido pela *Microsoft*. A empresa possui uma filial brasileira, sediada em São Paulo e, em reunião com o Ministério Público Federal de São Paulo, disse que, "a título de colaboração", encaminha as ordens judiciais de quebra de sigilo de dados telemáticos à sua matriz americana, para atendimento. Nem sempre, porém, esse atendimento é feito com presteza. Além disso, a empresa não faz interceptações de dados telemáticos (o "grampo" de e-mails), pois alega que a legislação americana não autoriza essa medida. Sugerimos que as ordens judiciais de quebra de sigilo de dados telemáticos continuem a ser enviadas às filiais nacionais desses provedores.

4.2.5. Interceptação de e-mails.

Medida muito útil para identificar os autores de um delito cibernético e também para comprovar a materialidade delitiva, a interceptação de dados telemáticos está prevista na Lei 9.296/96.

Os requisitos, prazo e procedimento da interceptação de dados telemáticos são os mesmos aplicáveis à interceptação das comunicações telefônicas. Sugerimos que o Ministério Público ou a autoridade policial requeiram a criação de uma "conta-espelho", isto é, uma conta de *e-mail* que contenha todas as correspondências eletrônicas recebidas e enviadas pelo usuário investigado. Com essa providência, a autoridade responsável pela investigação poderá monitorar, em tempo real, as comunicações eletrônicas feitas pelo usuário investigado. Sugerimos, ainda, que o provedor seja compelido a entregar, ao final da interceptação, uma mídia não-regravável

(CD-R) contendo todos os e-mails recebidos e enviados, eventuais arquivos anexados e todos os *logs* gerados no período (ver modelo anexo).

"Pescando" o criminoso com um e-mail "isca".

Quando dispomos apenas de um endereço eletrônico fornecido por um provedor estrangeiro, a identificação do usuário pode ser muito difícil. Um expediente simples, mas algumas vezes eficiente, é o envio de um *e-mail* "isca" ao usuário que se pretende identificar. O objetivo da isca é obter uma resposta eletrônica do investigado, pois será a partir dela que a identificação do usuário poderá ser feita (ver item 4.2). Numa investigação de um crime de racismo, por exemplo, o investigador poderá se mostrar interessado nas idéias divulgadas pelo autor da mensagem racista, e solicitar dele mais informações.

É óbvio que a linha telefônica usada para enviar o e-mail isca não pode pertencer a um órgão envolvido na persecução penal (pois o destinatário tem, como vimos, condições de identificar o provedor e a concessionária de telefonia usados pelo remetente); e também é evidente que o e-mail "isca", do remetente deve ser criado com essa finalidade específica e pertencer, de preferência, a um provedor estrangeiro (o próprio *Hotmail*, por exemplo), para dificultar a identificação.

4.3. SOFTWARES P2P (*KAZAA*, *E-MULE*, *E-DONKEY* ETC).

As conexões "peer-to-peer" (ponto-a-ponto) não possuem um provedor central de conexão: elas utilizam diversos servidores independentes e espalhados pela rede. Os arquivos trocados ficam armazenados nas estações dos usuários que participam da "rede", os servidores apenas fazem a "ponte" entre a pessoa que disponibiliza o arquivo e aquela que o quer baixar.

A estrutura garante a anonimidade dos usuários e servidores que participam da troca. A tecnologia P2P é usada nos aplicativos *Kazaa*, *GnuTella*, *e-Donkey*, *AudioGalaxy*, *Morpheus* e *BitTorrent*, dentre outros, para trocar arquivos de música (MP3), vídeo e imagem. As gravadoras alegam que a prática viola direitos autorais. Há a possibilidade de troca de qualquer tipo de arquivos, inclusive filmes e imagens contendo pornografia infantil.

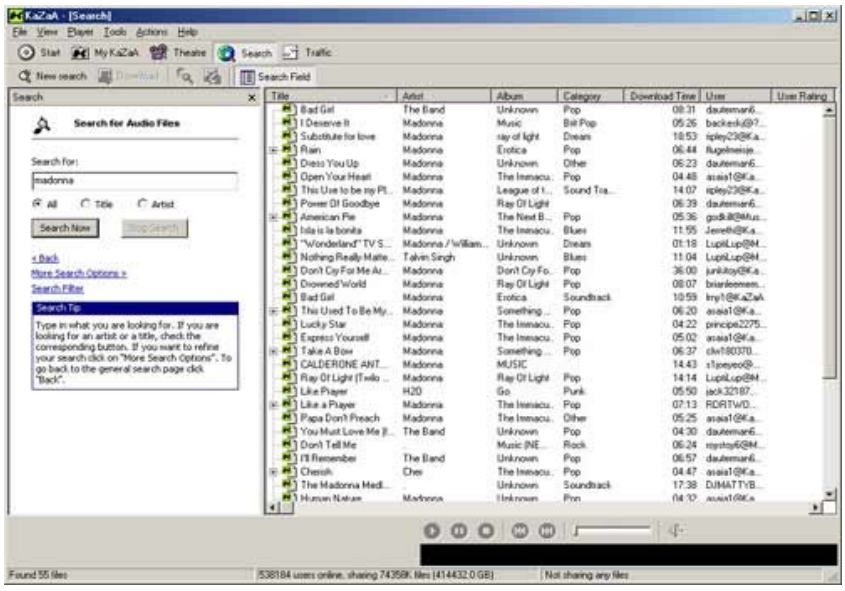
Novas versões do Kazaa impedem rastreamento

Novas versões independentes do Kazaa, software de compartilhamento de arquivos, impedem o rastreamento de seus *downloads*.

As versões são o Kazaa Lite 2.4.0 e o Kazaa K+++ 2.4.0 e prometem bloquear qualquer tipo de tentativa de rastreamento de seus *downloads*. Os autores criaram opções para desabilitar funções que permitem que um usuário veja todos os arquivos pertencentes a outros, sem contar que não salvam o histórico das pesquisas realizadas.

A autenticação de um usuário é feita por servidores gerenciados, normalmente, por comunidades anônimas, sediadas em países que não adotam legislações rígidas de uso da Internet. Os registros dos *logs* gerados, por serem imensos, não são armazenados. Além disso, na prática, quando um servidor P2P é fechado, outros rapidamente são criados, em qualquer parte do mundo.

Abaixo uma tela do software KAZAA, disponibilizando e procurando novos arquivos:



Infelizmente, o rastreamento das trocas de arquivos entre usuários desses sistemas é bastante difícil. Uma alternativa pode ser a identificação de um arquivo disponível em um computador de um usuário. O processo pode ser demorado, pois as indicações normalmente são vagas (como o simples nome do arquivo ou algumas palavras-chave pelas quais ele pode ser encontrado). É preciso, ademais, aguardar que o usuário denunciado faça a conexão à rede e disponibilize o arquivo para todos. Uma

vez localizado, o arquivo deve ser baixado para um computador onde possa ser analisado. Uma vez constatado o delito pode-se utilizar os dados colhidos durante a transferência para localizar o usuário e identificar seu IP (e ainda ter a hora da conexão já que o arquivo foi baixado em ambiente controlado). Algumas redes P2P são construídas de forma a garantir o anonimato do usuário, o que praticamente impede a identificação do criminoso sem que haja a colaboração do servidor.

4.4. MENSAGENS INSTANTÂNEAS (ICQ, MSN MESSENGER ETC.).

Os programas de mensagens instantâneas surgiram em 1996, com o ICQ, aplicativo criado pela empresa israelense *Mirabilis*. A idéia básica era (e ainda é) tornar mais ágil a comunicação entre os usuários da rede. A vantagem desses programas, em relação aos aplicativos de *e-mail*, é que eles permitem saber se um interlocutor qualquer está *online* e, com isso, trocar mensagens em tempo real.

Depois do ICQ, outros programas semelhantes surgiram. O provedor americano *America Online* criou o AIM (*AOL Instant Messenger*), mas depois acabou comprando a *Mirabilis*, fabricante do ICQ. A Microsoft e o Yahoo também lançaram seus produtos.

Feita a assinatura do serviço (gratuita), o usuário recebe um código que o identificará dentro da rede de usuários daquele programa de mensagens instantâneas. O código pode ser um número, um apelido ou um endereço de e-mail, dependendo do programa usado.

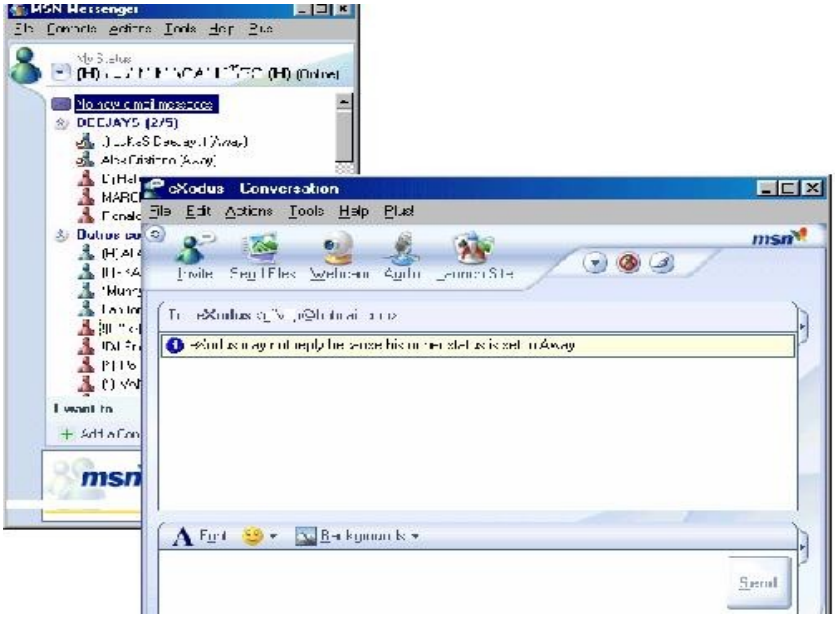
Depois de instalado o programa e configurada a conta, o usuário está apto a se comunicar com outras pessoas que assinam o mesmo serviço, desde que previamente cadastradas pelo usuário.

Quando um usuário tenta se comunicar com um contato de sua lista, o programa avisa o destinatário (por meio de um som ou de ícone) de que existe uma mensagem para ele. Uma janela, então, é aberta, e os interlocutores iniciam o diálogo.

4.4.1. Evidências necessárias.

Se a notícia do fato criminoso fizer referência a esses programas, o denunciante deverá providenciar a impressão ou salvar os dados de algum conversa ou do conteúdo da mensagem, e também dos dados dos interlocutores (números identificadores, apelidos ou *e-mail*), e ainda anotar a data e horário da comunicação.

Abaixo uma tela do MSN Messenger com uma tela de *chat* aberta:



4.4.2. Localizando o interlocutor de um “instant messenger”.

Antes de qualquer coisa é preciso verificar a forma como o aplicativo faz a autenticação na rede. Se for o ICQ, há um número, chamado UIN (*Universal Internet Number*). O *MSN* e o *Yahoo Messenger* utilizam um endereço de e-mail para fazer a autenticação na rede.

Para localizar o e-mail de um usuário do MSN Messenger, selecione o nome ou apelido do mesmo, clique com o botão invertido do mouse e localize a opção “propriedades”. Será aberta uma janela contendo o e-mail e dados do usuários do MSN.

De posse do UIN (ou do e-mail de autenticação) é preciso entrar em contato com o provedor do programa (o ICQ é mantido pela *American OnLine*; o MSN, pela *Microsoft*, o *Yahoo Messenger*, pela *Yahoo*) e solicitar o IP usado na data e horário anotados.

Com o IP em mãos, localiza-se o provedor (ou operadora de telefonia) e solicita-se a ele os dados do usuário. O procedimento é o mesmo que aquele descrito nos itens 4.1.6 e 4.1.7[11].

Existem ferramentas de rastreamento e localização de IP’s em aplicativos de Mensagens Instantâneas, mas os mesmos só podem ser usados quando a conversa está ocorrendo em tempo real, ou seja, é necessário estar com uma conexão ativa com o suspeito durante esta coleta de informação.

[11] Sobre a Microsoft, ver a observação do último parágrafo do item 4.2.4.

4.5. **SALAS DE BATE-PAPO (*CHATS*).**

As salas de bate-papo são uma outra forma de conversar com alguém, em tempo real, pela Internet. Os aplicativos mais novos permitem a criação de "salas virtuais", nas quais os usuários podem trocar mensagens e arquivos. Essas "salas" ficam hospedadas na própria *web*, diversamente do que ocorre com os programas de *messenger*. Não é necessário, por isso, fazer o *download* de aplicativos específicos: basta que o usuário forneça seu nome ou apelido (*nickname*).

Temos recebido notícias de adultos que usam as salas de bate-papo disponibilizadas pelos grandes provedores nacionais para atrair e seduzir crianças, ou, então, para trocar fotos e vídeos contendo pornografia infantil. Para combater esse tipo de crime, a polícia inglesa desenvolveu um programa de detecção de pedófilos em salas de *chat*, apelidado justamente de "*chatnannie*". O programa usa recursos da inteligência artificial para "entrar" em uma sala de bate-papos e dar a impressão de que a conversa se realiza com uma criança; ao mesmo tempo, o aplicativo analisa as respostas e o comportamento do interlocutor e informa as autoridades policiais, caso haja alguma conversa "suspeita".

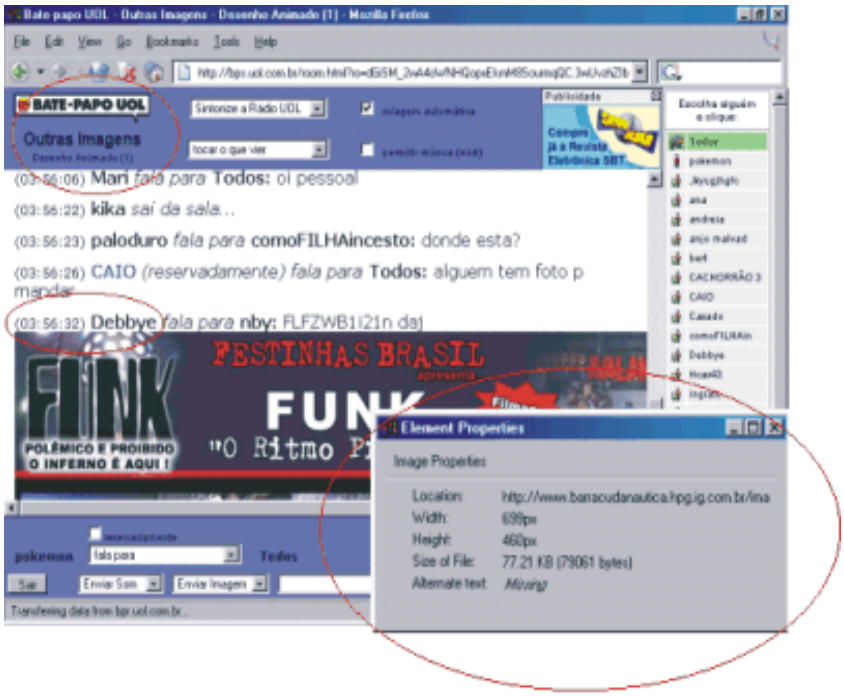
4.5.1. Evidências necessárias.

Quando o usuário tomar conhecimento de um delito eletrônico praticado em uma sala de bate-papo, deverá salvar ou imprimir o conteúdo da conversa, e também anotar todos os dados disponíveis sobre o *chat*, tais como o *site* onde o serviço funciona, o nome de sala, os *nicknames* usados e a data e a hora em que houve a conversa.

Nos *chats* que permitem a troca direta de imagens, recomendamos que o usuário capture os dados da imagem, clicando em cima dela com o botão invertido do mouse e escolhendo a opção "propriedades". Imprima ou salve esta tela e anexe-a aos outros dados coletados. Apresentamos, abaixo, uma tela que contém os dados de uma imagem trocada num *chat*:

4.5.2. **Identificando o autor de uma mensagem em um *chat*.**

Provedores nacionais com maior estrutura de armazenamento, costumam manter *logs* dos *chats* ocorridos em seu domínio. De posse do apelido do investigado e da data e do horário em que ocorreu a conversa, a autoridade policial ou o Ministério Público deverá requerer judicialmente a quebra do sigilo de dados telemáticos, para que o provedor forneça o IP gerado quando do acesso do investigado na sala de bate-papo. O procedimento é o mesmo que aquele descrito nos itens 4.1.6 e 4.1.7.



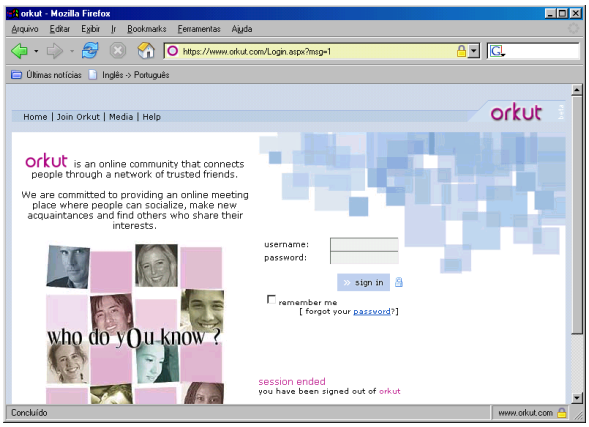
4.6. LISTAS DE DISCUSSÃO.

As listas (ou grupos) de discussão – hospedadas, por exemplo, no “Yahoo! Groups” ou no “Grupos.com.br” - utilizam o e-mail para a troca de mensagens entre os integrantes de um determinado grupo temático. Existem milhares de listas hospedadas na Internet, sobre os mais variados assuntos, alguns deles criminosos (grupos nazistas, por exemplo).

Para participar de um grupo, o usuário deverá assinar a lista e acompanhar a discussão apenas como leitor ou contribuindo com comentários. Alguns grupos são moderados, isto é, contam com uma pessoa que decide quem participará da lista e quais as mensagens poderão ser publicadas.

Como o meio utilizado por essas listas para a troca de mensagens é o endereço eletrônico, a investigação deve seguir os passos descritos no item 4.2., ou seja, o usuário deverá localizar o cabeçalho de e-mail do responsável por alguma mensagem e deste localizar o IP de origem da mensagem.

4.7. ORKUT.



O ORKUT (www.orkut.com) é uma comunidade virtual de relacionamentos, criada em 22 de janeiro de 2004 e mantida pela empresa GOOGLE. Possui atualmente mais de 13 milhões de membros, sendo 72% deles brasileiros. Comparando com os dados fornecidos pelo Comitê Gestor da Internet no Brasil[12], podemos concluir que de cada 10 internautas brasileiros, 3,1 estão cadastrados no Orkut. Apesar da empresa mantenedora do serviço proibir o cadastro de menores de idade, há dezenas de milhares de crianças e adolescentes inscritos na comunidade de relacionamentos.

Infelizmente o ORKUT vem abrigando centenas de sub-comunidades criminosas, nas quais é possível comercializar drogas, divulgar idéias intolerantes e encontrar pornografia infantil. A maioria das notícias que temos recebido referem-se a comunidades racistas e nazistas.

Até julho de 2005, a empresa americana Google não possuía filial no Brasil, o que dificultava imensamente a identificação de usuários criminosos. Após diversos “convites” não atendidos, o representante legal da empresa finalmente resolveu colaborar, e desde março de 2006 temos encaminhado à Justiça Federal pedidos de quebra de sigilo de dados telemáticos, para a obtenção dos dados cadastrais, logs de acesso, e cópias em papel e em meio magnético dos perfis e comunidades investigados. Também propusemos à empresa a assinatura de um termo de compromisso semelhante ao já celebrado com os provedores de acesso.

4.7.1. Evidências necessárias.

[12] Segundo o CGI-BR cerca de 32,2 milhões de brasileiros com mais de 16 anos tem acesso a internet. <http://www.nic.br/indicadores/usuarios/tab02-05.htm>

Os crimes no serviço Orkut podem ser praticados nas comunidades virtuais e nas páginas contendo os perfis dos usuários. São exemplos da segunda situação a publicação de perfis falsos, com conteúdo difamatório, e a veiculação, nos álbuns associados aos perfis, de imagens e fotografias de crianças em cenas sexuais. As comunidades virtuais são usadas para reunir usuários com as mesmas preferências, sejam elas lícitas ou ilícitas. A cada dia, são criadas centenas de novas comunidades temáticas, muitas delas com o fim de disseminar a intolerância, em todas as suas manifestações.

Quando o usuário tomar conhecimento de uma conduta criminosa praticada em ambientes do serviço Orkut, deverá salvar ou imprimir o conteúdo da comunidade, mensagem ou imagem ofensiva, e também da página inicial do usuário responsável por aquele conteúdo.

4.7.2. Identificando o autor de um crime praticado no Orkut.

De posse das evidências acima referidas, o investigador deverá requerer judicialmente a quebra do sigilo de dados telemáticos, para que a empresa GOOGLE BRASIL, responsável pelo serviço, forneça os logs de acesso, e cópias em papel e em meio magnético dos perfis e comunidades investigados (os dados da empresa estão no anexo II). O procedimento é o mesmo que o descrito nos itens 4.1.6 e 4.1.7.

4.8. PROXY.

Até agora, tratamos das operações usuais de acesso à Internet, mas é necessário dizer que nem sempre o usuário realiza a conexão direta com o website, cliente de e-mail, salas de bate-papo e os demais serviços disponíveis na rede mundial.

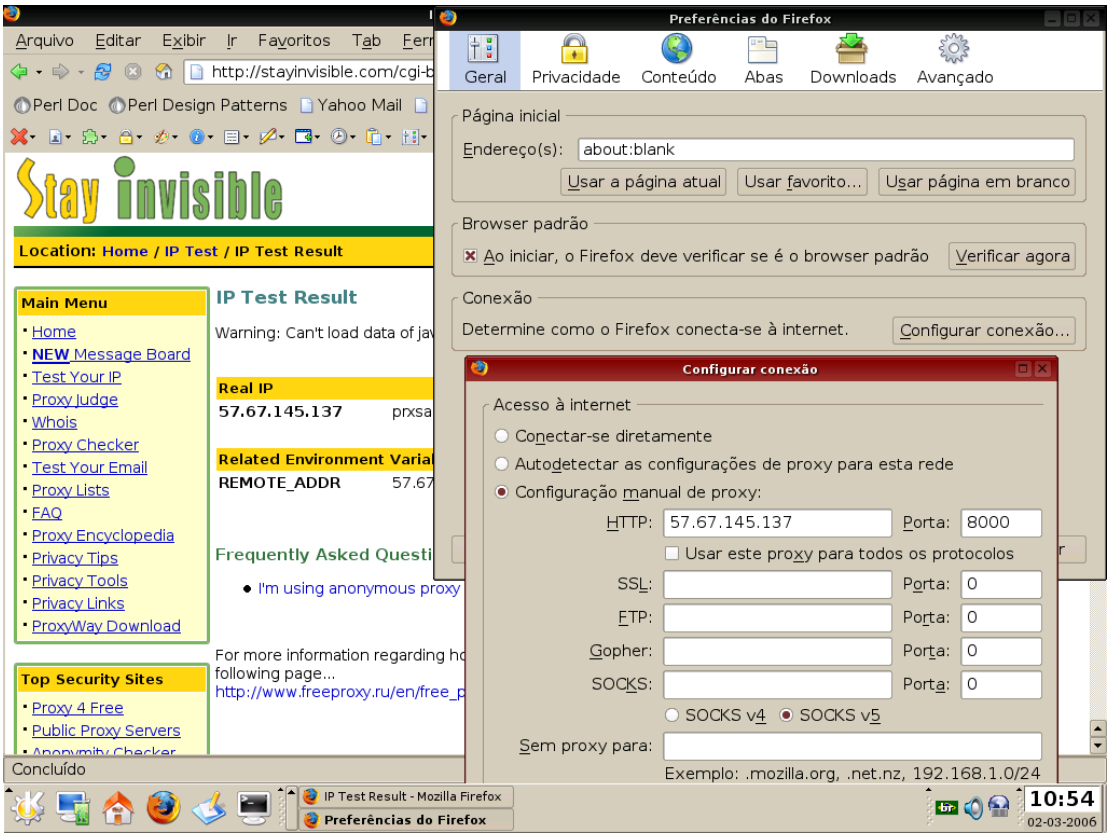
Com efeito, o usuário pode optar por utilizar um método de acesso indireto, que funciona da seguinte maneira: o usuário se conecta a um servidor específico, que lhe serve de “ponte” para acessar o verdadeiro conteúdo desejado. O servidor conectado utiliza um IP próprio e “esconde” o IP original do usuário, de forma que toda mensagem que chega no servidor é redirecionada a usuário e toda mensagem que parte do usuário é identificada apenas pelo IP do servidor. Este tipo de serviço chama-se *Proxy*.

Para nós, o maior problema é que há na Internet[13] servidores Proxy que garantem ao usuário o anonimato do IP de acesso, e ainda muitos programas gratuitos para fazer as configurações necessárias à utilização dessa forma de acesso indireto à rede. Há ainda a possibilidade do usuário se utilizar de múltiplos servidores Proxy, de forma a dificultar ainda mais o

[13] Uma lista deles pode ser obtida nos endereços www.publicproxyservers.com e www.stayinvisible.com – horário do acesso 22:41 27/02/06 -3:00 GMT.

rastreamento.

De todo o modo, a identificação do usuário depende da colaboração dos servidores Proxy envolvidos. Abaixo, a tela de um serviço Proxy que promete anonimato ao usuário:



A real função dos servidores de Proxy

Os servidores Proxy não se prestam, apenas à prática de crimes. A maioria deles busca legitimamente “esconder” o IP do usuário, a fim de protegê-lo contra técnicas maliciosas de invasão, roubo de dados e envio de spams.

O Proxy serve também para negar ao usuário o acesso a listas de IPs bloqueados (é o que ocorre na maioria das máquinas ligadas à rede MPF) e para armazenar cópia de sites, de forma a facilitar o acesso pelo internauta.

5. COMPETÊNCIA JURISDICIONAL NOS CRIMES CIBERNÉTICOS.

Como vimos no item 3, são muitas as condutas delituosas que podem ser praticadas por meio da Internet. É preciso, então, definir quais os tipos penais estão sujeitos ao processamento e julgamento pela Justiça Federal.

Nos termos do artigo 109, inciso IV, da Constituição brasileira, compete aos juízes federais processar e julgar os crimes cometidos em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Assim, é competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso. Podemos citar, a título exemplificativo, o estelionato eletrônico[14], o dano ou a falsificação de dados constantes em sistemas informatizados mantidos por órgão ou entes da administração pública federal.

Quanto à hipótese prevista no inciso V do artigo 109 da Constituição, ou seja, os crimes previstos em tratado ou convenção internacional, quando iniciada a execução no país o resultado tenha ou devesse ter ocorrido no estrangeiro, vale lembrar que as condutas tipificadas no artigo 241 do Estatuto da Criança e do Adolescente e também o crime de racismo (tipificado na Lei 7.716/89) têm previsão em convenções internacionais de direitos humanos. Como a consumação delitiva normalmente ultrapassa as fronteiras nacionais quando os dois crimes são praticados através da Internet, a competência para julgá-los pertence à Justiça Federal.

No que tange à pornografia infantil, o Decreto Legislativo nº 28, de 24.09.90, e o Decreto Presidencial nº 99.710, de 21.11.90, incorporaram ao direito pátrio a *Convenção da ONU sobre os Direitos da Criança*. A Convenção obriga os Estados-Partes, dentre outras medidas, a: a) dar proteção legal à criança contra atentados à sua honra e à sua reputação (art. 16); b) tomar todas as medidas que forem necessárias para proteger a criança contra todas as formas de exploração e violência sexual, inclusive para impedir que seja explorada em espetáculos ou materiais pornográficos (art. 34). Ressalte-se que referida Convenção prevê expressamente o comprometimento dos Estados em adotar medidas de natureza legislativa para a proteção dos direitos da criança (art. 4º).

A competência da Justiça Federal para processar e julgar a divulgação na Internet de material pornográfico envolvendo crianças e adolescentes já foi reconhecida por quatro Tribunais Regionais Federais (1ª, 3ª, 4ª e 5ª Regiões) brasileiros. As ementas dos acórdãos estão no anexo I deste manual. Esses acórdãos reconheceram presente o requisito da extraterritorialidade, uma vez que a visualização de imagens de pornografia

[14] Recebemos, uma vez, a notícia de que uma advogada transmitia, pela Internet, declarações de imposto de renda ideologicamente falsas, com o objetivo de receber, em nome de "laranjas", restituições indevidas de imposto de renda. Trata-se de um caso evidente de estelionato eletrônico, praticado contra a Receita Federal.

infantil publicadas na Internet pode, virtualmente, ocorrer em qualquer país do mundo.

Também está sujeito à competência da Justiça Federal o crime de racismo, tipificado na Lei Federal n.º 7.716/89, já que a discriminação racial é prática vedada pela *Convenção sobre a eliminação de todas as formas de discriminação racial*, ratificada pelo Brasil em 1968 e vigente no território nacional a partir da edição do Decreto Presidencial n.º 65.810, de 8.12.1969. A Convenção obriga os Estados-partes a: *a)* não encorajar, defender ou apoiar a discriminação racial praticada por uma pessoa ou uma organização qualquer (art. 2º, § 1º, "b"); b) tomar todas as medidas apropriadas, inclusive, se as circunstâncias o exigirem, medidas de natureza legislativa, para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupo ou organização (art. 2º, § 1º, "d"); c) declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento (art. 4º, "a"). Portanto, os chamados "crimes de ódio", quando praticados por meio da Internet, também são da atribuição da Justiça Federal.

Outros delitos não abrangidos pelas hipóteses acima mencionadas – por exemplo, os crimes contra a honra de particular, praticados através da rede - deverão ser investigados e processados no âmbito das Justiças Estaduais, já que o simples fato do crime ter sido cometido por meio da Internet não é suficiente para justificar a competência da Justiça Federal.

6. A RESPONSABILIDADE DOS PROVEDORES.

A legislação brasileira sobre a responsabilidade dos provedores no enfrentamento aos crimes cibernéticos é manifestamente deficiente, uma vez que não há, em nosso ordenamento, a definição clara dos deveres das empresas que mantém serviços de acesso e hospedagem de páginas em matéria criminal.

Em países mais empenhados no combate à essa modalidade delitiva - como por exemplo Holanda, Suécia, Austrália e Canadá – os governos estão exigindo dos provedores que informem a polícia ou o Ministério Público tão logo tomem conhecimento de crimes cometidos no uso dos serviços de Internet, e também que preservem as evidências necessárias à investigação criminal, por um prazo mínimo estabelecido por lei.

Como já vimos, a identificação de um criminoso cibernético depende, em grande medida, da identificação do endereço IP do computador por ele utilizado. Um provedor de acesso normalmente controla uma gama de centenas ou milhares de endereços de IP, os quais são atribuídos aos assinantes, durante o período de conexão.

Os números de IP são normalmente dinâmicos, ou seja, cada vez que um usuário faz a conexão à rede por meio de um provedor de acesso, seu computador é aleatoriamente vinculado a um endereço de IP, disponibilizado pelo provedor. O computador do usuário retém o endereço de IP pela duração da conexão, impedindo que o mesmo protocolo seja atribuído a outro assinante, no mesmo período. Quando, porém, o usuário encerra a conexão, o protocolo torna-se novamente disponível para ser atribuído a outro assinante. Assim, um endereço de IP de dado usuário normalmente difere a cada vez que ele se conecta por meio de algum provedor, e um dado endereço de IP poder estar associado a centenas ou milhares de diferentes usuários por um período de semanas ou meses.

Para que seja possível identificar qual usuário estava ligado a determinado endereço de IP, num determinado dia e hora, os provedores de acesso e também de hospedagem devem manter um banco de dados eletrônico, uma lista de cada endereço de IP utilizado, juntamente com a correspondente data, horário e região de conexão. A *International Association of Prosecutors* recomenda que os provedores mantenham os *logs* de acesso pelo prazo mínimo de um ano, de forma que, quando forem formalmente requisitados, tenham disponível a informação de interesse do órgão solicitante, inclusive para instruir os casos envolvendo cooperação internacional, em cujo âmbito as investigações demandam maior tempo para sua conclusão.

É indispensável que os provedores proporcionem, ainda, a educação necessária ao uso responsável da Internet. É cada vez mais precoce o uso, pelas crianças, da rede mundial de computadores, sendo certo que elas estão muito expostas ao assédio de criminosos. Considerando, ainda, que a repressão penal é insuficiente para coibir as

práticas nocivas mais comuns da Internet, é imprescindível que os provedores assumam a responsabilidade de informar corretamente os consumidores de seus serviços acerca dos mecanismos de proteção contra ações danosas.

Como já foi dito, a Lei 10.764/03 previu explicitamente a responsabilidade criminal dos administradores e empregados de pro*vedores, quando estes: a) assegurarem os meios ou serviços para o armazenamento das fotografias ou imagens de crianças ou adolescentes em cena de sexo explícito; b) assegurarem, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, das fotografias, de tais cenas ou imagens.*

À míngua de uma legislação mais abrangente, algumas unidades do Ministério Público Federal – incluindo a nossa - têm celebrado "termos de compromisso" com os provedores locais, objetivando fazer com que eles:

a) divulguem campanhas contra a pornografia infantil e contra os crimes de ódio;

b) orientem o público sobre a utilização não criminosa de salas de bate-papo, grupos e fóruns de discussão, *blogs*, páginas pessoais e outros serviços disponibilizados ao usuário;

c) insiram, nos instrumentos de adesão ao serviço, cláusula que preveja a rescisão do contratual na hipótese do usuário valer-se do provedor para veicular fotografias e imagens de pornografia infantil, ou idéias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação;

d) mantenham *link* pelo qual os usuários possam noticiar ao provedor signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum eletrônico, ou outro serviço prestado pelo próprio provedor;

e) informem imediatamente ao Ministério Público Federal, quando tomem conhecimento de que abrigam pornografia infantil ou conteúdo manifestamente discriminatório, assegurada a proteção ao sigilo dos dados telemáticos;

f) preservem e armazenem, pelo prazo mínimo de 6 (seis) meses, o registro de *logs* de acesso discado e, quando possível, também os IPs originários dos usuários dos serviços de *web page*, salas de bate-papo, *fotologs*, fóruns de discussão *on-line* e outros.

g) solicitem e mantenham os dados cadastrais informados por seus assinantes de acesso;

h) exijam que os novos usuários informem o número de algum documento validável de identificação, como por exemplo o número do RG ou do CPF.

Como se vê, o objetivo do termo é comprometer os provedores no combate aos crimes de pornografia infantil e racismo, quando cometidos através da Internet.

Inclusive sob o aspecto ético, a responsabilidade dos provedores em zelar pela não disseminação de tais práticas é algo incontestável, visto que, uma vez hospedando conteúdos de pornografia infantil, os provedores contribuem, em muito, para o convencimento do público em geral, inclusive crianças, muitas delas já usuárias da Internet, de que a pornografia infantil e a exploração sexual de crianças e adolescentes é algo natural, divertido e prazeroso.

Nesse sentido, a cooperação entre os Provedores de Acesso à Internet e as autoridades responsáveis pelo combate à pedofilia e ao racismo é indispensável para o bom êxito das investigações e da persecução penal.

De outra forma, provedores que, uma vez obrigados judicialmente a fornecer determinada informação ou proceder à determinada conduta, deliberadamente deixarem de fazê-lo devem ser sancionados na forma como a legislação estabelecer, na medida em que se tornam partícipes e assistentes na disseminação da pornografia infantil.

Por fim, cumpre observar que, em razão da Internet ser um sistema que pode ser acessado internacionalmente, os esforços para o combate à exploração sexual e às práticas de racismo devem igualmente ser amplos no seu escopo, envolvendo não apenas os órgãos encarregados da persecução e aplicação da lei penal, como também a cooperação de outros segmentos do setor público e privado.

ANEXO I:
JURISPRUDÊNCIA RECOLHIDA

1. Art. 241 do ECA. Crime praticado pela Internet. Competência da Justiça Federal:

- "PENAL E PROCESSUAL PENAL. HABEAS CORPUS. TRANCAMENTO DE AÇÃO PENAL. COMPETÊNCIA DA JUSTIÇA FEDERAL. DENEGAÇÃO DA ORDEM. 1. A divulgação de fotos pornográficas de menores na internet é crime previsto em convenção internacional, o que firma a competência da Justiça Federal para o seu processamento, independentemente do resultado ter ou não ocorrido no estrangeiro (artigo 109, v, da Constituição Federal). 2. Denegação da ordem." (TRF – 5ª Região – HC 2002.05.00.013765-0 – Rel. Des. Ricardo César Mandarino Barretto – j. 25.06.02 – DJU 03.10.02, p. 600).
- "PENAL. ESTATUTO DA CRIANÇA E DO ADOLESCENTE (LEI 8.069/90). ARTIGO 241. COMPETÊNCIA DA JUSTIÇA FEDERAL. ART. 109, V, DA CF/88. CONVENÇÃO DOS DIREITOS DA CRIANÇA. DECRETO LEGISLATIVO Nº 28/90 E DECRETO Nº 99.710/90. (...) DIVULGAÇÃO DE IMAGENS PORNOGRÁFICAS DE MENORES PELA INTERNET. (...) 1. O Congresso Nacional, através do Decreto Legislativo nº 28, de 24.09.90, bem como o Governo Federal, por força do Decreto nº 99.710, de 21.11.90, incorporaram ao direito pátrio os preceitos contidos na Convenção Sobre os Direitos da Criança, que prevê, entre outras coisas, que os Estados Partes darão proteção legal à criança contra atentados à sua honra e a sua reputação (art. 16), bem como tomarão as medidas que foram necessárias para impedir a exploração da criança em espetáculos ou materiais pornográficos (art. 34). 2. A Justiça Federal é competente para o processamento e julgamento da causa, aplicando-se à hipótese o disposto no art. 109, V, da CF/88, pois o delito praticado (art. 241 do ECA) encontra previsão no citado tratado, bem como sua execução teve início no País. Quanto ao resultado, levando-se em conta que o meio de divulgação utilizado foi a rede mundial de computadores (INTERNET), as fotos podem ter alcançado todos os países que tem conexão com a rede, ou seja, praticamente todo o planeta. 3. Tendo o réu se conformado com a decisão que lhe negou a suspensão do processo, não é possível, já em fase recursal, quando toda a instrução probatória já foi realizada, bem como todos os atos processuais, se falar em suspender o processo. Preliminar não conhecida por se tratar de questão preclusa. 4. Comprovadas a materialidade e a autoria do delito pelo farto conjunto probatório, é de ser reconhecida a responsabilidade penal do réu pelo cometimento do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente, pois o mesmo utilizava-se de seu site na Internet para divulgar pornografia infantil, através da publicação de fotos pornográficas envolvendo crianças,

que eram enviadas a ele por correio eletrônico (e-mail).” (TRF – 4ª Região – ACR 2002.04.01.03.3189-7 – Rel. Juiz José Luiz B. Germano da Silva – j. 29.04.03 – DJU 21.05.03, p. 806).

- CONSTITUCIONAL. PROCESSUAL PENAL. CONDENAÇÃO PELOS DELITOS DOS ARTIGOS 241 DA LEI Nº 8.069/1990 E 218 DO CÓDIGO PENAL. “HABEAS CORPUS”. TESE DE INCOMPETÊNCIA DA JUSTIÇA FEDERAL. ARTIGO 109-V, DA CONSTITUIÇÃO FEDERAL. INCONSISTÊNCIA. 1 – Ao contrário do que afirma o impetrante, a denúncia atribui ao paciente dolo direto na realização do tipo, sendo certo que, ao consumar o crime, publicando, na Internet, fotografias, contendo cenas pornográficas de sexo explícito, envolvendo crianças e adolescentes, deu causa ao resultado da publicação legalmente vedada, dentro e fora dos limites do território nacional, justificando a incidência do artigo 109-V, da Constituição Federal, sem espaço para, na espécie, cogitar-se de situação de mero exaurimento do delito, quando o que se tem é sua efetiva concretização, dentro e fora do País. 2 – Irrelevância de precedente do Colendo STF para balizar o deslinde da causa. 3 – Ordem denegada.” (TRF – 1ª Região – Rel. Juiz Hilton Queiroz – HC 2001.01.00.029296-8/GO – j. 28.11.01).

- “O Decreto Legislativo n.º 28, de 24.09.90 e o Decreto n.º 99.710, de 21.11.90 incorporaram ao direito pátrio os preceitos contidos na Convenção Sobre os Direitos da Criança que prevê que os Estados darão proteção legal à criança contra toda forma de exploração, inclusive abuso sexual (art. 19), bem como tomarão as medidas que forem necessárias para impedir a exploração da criança em espetáculos ou materiais pornográficos (art. 34). Assim estando o delito praticado (artigo 241 do Estatuto da Criança e do Adolescente) previsto no citado tratado aplica-se à hipótese o disposto no artigo 109, V, da Constituição Federal. (...) Além disso, não obstante a execução ter se iniciado no Brasil, o resultado produziu efeitos extraterritoriais, em razão da divulgação de fotos pornográficas de menores pela rede mundial de computadores (Internet) que alcança todos os países a ela conectados. (...) Consoante ainda observado pelo *Parquet* Federal *“...em conformidade com o art. 21, inciso XI, da Constituição Federal Brasileira, a exploração de serviços de telecomunicação é de competência exclusiva da União, do qual se infere o interesse da União nos delitos praticados por meio da Internet, sendo, portanto, a competência da Justiça Federal resguardada também com fundamento no art. 109, inc. I da Constituição Federal”* (fl. 49). (TRF – 3ª Região – RESE 2003.61.81.000927-6 – Rel. Des. Vesna Kolmar – j. 30.11.04).

2. Art. 241 do ECA. Crime praticado pela Internet. Tipicidade.

- "Crime de Computador: publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada - é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá- la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial" (STF – 1ª Turma - HC 76.689/PB – Rel. Min. Sepúlveda Pertence – j. 22.09.98 – DJU 06.11.98, p. 03).
- "O cerne da questão em debate é saber se a conduta praticada pelo paciente na vigência da antiga redação do art. 241 do Estatuto da Criança e do Adolescente corresponde ao núcleo do tipo, o verbo "publicar". (...) Sustenta o impetrante que o paciente, ao trocar arquivos pela internet, o fez em uma sala de bate-papo reservadíssima (acesso restrito) e com apenas uma pessoa, o que não corresponderia ao verbo "publicar" exigido pelo tipo. Assim não me parece. O verbo constante do tipo do art. 241 do ECA está intimamente ligado à divulgação e reprodução das imagens de conteúdo sexual ou pornográfico envolvendo crianças e adolescentes, no sentido de torná-las públicas. Qualquer meio hábil a viabilizar a divulgação dessas imagens ao público em geral corresponde ao que o legislador almejou com a utilização do verbo "publicar". Neste sentido, já dizia Nélson Hungria que publicar significa "tornar público, permitir o acesso ao público, no sentido de um conjunto de pessoas, pouco importando o processo de publicação" (Comentários ao Código Penal. Rio de Janeiro: Forense, 1958. Vol. VII. p. 340). Não resta dúvida de que a internet é um veículo de comunicação apto a tornar público o conteúdo pedófilo das fotos encontradas, o que já demonstraria, em tese, a tipicidade da conduta. Ademais, a denúncia formulada foi clara em registrar que qualquer pessoa que acessasse o servidor de arquivos criado pelo paciente teria à disposição esse material (...). Por outro lado, a discussão referente ao advento da Lei 10.764/2003 não

foi ventilada - e muito menos apreciada - no recurso em habeas corpus interposto no Superior Tribunal de Justiça, motivo por que não conheço do writ nessa parte, para evitar supressão de instância. Evidente que à época da redação do dispositivo original (1990), o legislador não teria como prever o surgimento dessa nova tecnologia, daí por que já se decidiu ser o tipo do art. 241 aberto. Não foi outra a razão de a doutrina e a jurisprudência terem assinalado que qualquer instrumento hábil a tornar público o material proibido estaria incluído na compreensão do verbo "publicar". Por isso não se pode falar em interpretação prejudicial ao paciente nem em aplicação da analogia *in malam partem*." (STF – 2ª Turma - HC 84561/PR - Rel. Min. Joaquim Barbosa – j. 5.10.2004 – DJU 26.11.04).

3. Interceptação de conversa em sala de bate-papo. Ausência de proteção constitucional ao sigilo.

- "A conversa realizada em 'sala de bate papo' da Internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais. (...) Dos documentos acostados é verificado que a INTERPOL interceptou conversa do acusado em 'sala de bate-papo' na Internet, momento em que foi noticiado a transmissão de imagens pornográficas envolvendo crianças e adolescentes. Esta conduta funcionou como elemento condutor da instauração do referido inquérito policial. (...) Acertada a decisão do e. Tribunal Regional Federal da 3ª Região que sobre o tema entendeu não haver o sigilo das comunicações, uma vez que a conversa fora realizada em 'sala de bate papo' da internet, em que se caracteriza, em 'ambiente virtual de acesso irrestrito e destinado a conversas informais'" (STJ – 6ª Turma – RHC 18.116-SP – Rel. Min. Hélio Quaglia Barbosa – j. 16.02.06).

ANEXO II:
PEÇAS PROCESSUAIS

1. Pedido de busca e apreensão de computadores. Crime de racismo praticado pela rede.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA 1ª VARA CRIMINAL FEDERAL DA SUBSEÇÃO JUDICIÁRIA DE SÃO PAULO.

Autos n.º XXXX (URGENTE)

O **MINISTÉRIO PÚBLICO FEDERAL**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência requerer, com fundamento no art. 240 e ss. do Código de Processo Penal, a expedição de

MANDADO DE BUSCA E APREENSÃO

nos seguintes termos:

Em 04 de junho último, a Comissão de Defesa do Consumidor, Meio Ambiente e Minorias da Câmara dos Deputados encaminhou ofício ao Diretor Geral do Departamento de Polícia Federal noticiando que o sítio http://www.kkkk.net/brazil contém textos e símbolos que incentivam a discriminação e o preconceito de raça e cor (fls. 04).

Instaurou-se o presente inquérito policial para apurar a conduta em questão, que está subsumida no art. 20, *caput* e § 2º, da Lei Federal n.º 7.716/89.

O sítio, consoante atesta o documento de fls. 06, é mantido por um provedor situado nos EUA. Uma parte de seu conteúdo pode ser vista a fls. 07-09. Há nele a menção a um **endereço eletrônico (**xxxxxx@hotmail.com**)**, e a uma **caixa postal** no Brasil (CP XXXX, CEP XXXXXX). Há também a referência a uma organização denominada "***Imperial Klans of Brazil – Knights of the Ku Klux Klan***".

Como é sabido, a "*Ku Klux Klan*" é uma nefasta organização criminosa criada no sul dos Estados Unidos logo após a Guerra Civil Americana. Pregava a superioridade da "raça" branca e foi responsável pela **morte de mais de mil e quinhentas pessoas**. Covardes que eram, seus membros trajavam capuzes para ocultar suas verdadeiras identidades. A

organização sobrevive, atualmente, graças ao fanatismo e à intolerância de uma minoria, pouco esclarecida.

Pois bem. Uma "mensagem-isca" foi enviada ao endereço eletrônico constante do sítio (XXXXX@hotmail.com). Uma pessoa, que se autodenominou "**BROTHER MARCOS 33/6**", respondeu o e-mail e, com isso, foi possível localizar o endereço IP usado pelo usuário no ato da resposta. O número obtido foi 200.171.77.132, e o acesso à rede mundial de computadores ocorreu no dia 24 de junho de 2003, às 13:33:47 (GMT).

Em atendimento a pedido formulado pelo Ministério Público Federal, este juízo ordenou a quebra do sigilo de dados telemáticos do número IP 200.171.77.132 e, com isso, foi possível identificar o **endereço a partir de onde foi feita a conexão com a rede mundial de computadores**. O endereço é **Rua XXXXXXX, 21**. O nome do assinante da linha é a empresa **XXXXXXXX**, de propriedade de **YYYYYYY** e XXXXXXXXXX.

A Polícia Federal apurou, também, que o destinatário da Caixa Postal n.º XXXX é **XXXXXXXX**, e o endereço fornecido é **Rua XXXXXX, 86**.

XXXXXXXX de fato reside nesse último endereço, consoante atestam os documentos ora anexados.

Nesse mesmo endereço está instalada a linha telefônica n.º (11) 5522-3378, de propriedade de YYYYYYY, consoante atesta a anexa informação, fornecida no sítio da companhia telefônica.

Há, portanto, indícios suficientes que YYYYYYYY e XXXXXXXXX mantêm algum tipo de relacionamento, e que um deles é o responsável pela publicação da página.

O sítio contendo o conteúdo racista ainda está publicado na rede. Há nele outras páginas que ainda não haviam sido juntadas aos autos.

Nelas, as mensagens de racismo são ainda mais evidentes. "**Acaso o senso comum nos diz que somos 100% perfeitamente iguais?**" ("Doesn't common sense tell us that we are all 100% perfectly equal?"), perguntam os membros dessa organização em uma das páginas ora anexadas. "**Olhe dentro dos olhos de uma criança *branca* e lembre-se dos motivos da criação deste grupo**", composto por "**arianos (homens brancos honráveis)**".

O objetivo do grupo é a "**defesa dos direitos da raça branca**[15]". "Queremos entender porque que os outros (*sic*) seres podem ter

[15] Celso Lafer, em parecer juntado aos autos do *habeas corpus* n.º 82.424-2, julgado pelo Supremo Tribunal Federal em setembro de 2003, lembra que a divisão dos seres humanos em raças é absolutamente insustentável do ponto de vista científico. "O avanço do conhecimento se incumbiu de mostrar que não há fundamento biológico em qualquer subdivisão racial da espécie humana e que os critérios das diferenças visíveis, a começar pela cor da pele, são apenas juízos de aparência. As diferenças genéticas individuais entre duas pessoas brancas são maiores que a diferença genética média entre brancos e negros e não custa lembrar que a integridade genética da espécie humana, como unidade, é comprovada na reprodução entre pessoas de 'raças' diferentes, gerando descendentes normais e férteis. (...) A capacidade de desvendar o genoma humano – que é uma revolução coperniquiana da biologia – permite dizer que conhecer uma espécie reduz a conhecer o seu genoma completo, e o seqüenciamento do genoma humano indica que as diferenças

direitos especiais e facilidades em conseguir uma vaga de emprego e lugares garantidos nas faculdades". "Gostaríamos de mostrar ao mundo os **verdadeiros problemas de uniões inter-raciais**". Somos informados, também, que "**o Ku Klux Klan salvou o mundo duas vezes**" e que "**os judeus são filhos do demônio**" – "**aqueles judeus que mataram o Senhor Jesus, que nos perseguiram, que não são do agrado de Deus, que são inimigos de todos os homens**". "**Os verdadeiros filhos de Deus são os brancos**, que tem a fé, o sangue e a honra de ter uma vida justa. Devemos defender o futuro de nossa raça, evitando que um novo holocausto seja originado".

A materialidade do delito tipificado no art. 20, *caput*, e § 2º, da Lei 7.716/89 está, como se vê, Excelência, perfeitamente demonstrada.

Há também indícios suficientes da autoria delitiva.

Todavia, o prosseguimento das investigações depende da apreensão dos computadores que contêm as páginas racistas, bem como de outros documentos e objetos que autorizem o ajuizamento da ação penal em face dos autores desse repugnante fato criminoso.

A competência para a autorização da medida ora requerida pertence à Justiça Federal, nos termos do disposto no art. 109, inciso V, da Constituição da República (*in verbis*: "aos juízes federais compete processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente").

Com efeito, o art. 4º da Convenção Internacional sobre a eliminação de todas as formas de discriminação racial (assinada pelo Brasil em 07 de março de 1966; ratificada, sem reservas, em 27 de março de 1968; e publicada através do Decreto Presidencial n.º 65.810, de 08 de dezembro de 1969), estabelece:

> **"Os Estados-partes condenam toda propaganda e todas as organizações que se inspiram em idéias ou teorias baseadas na superioridade de uma raça ou de um grupo de pessoas de uma certa cor ou de uma certa origem étnica ou que pretendam justificar ou encorajar qualquer forma de ódio e de descriminação raciais, e comprometem-se a adotar, imediatamente, medidas positivas destinadas a eliminar qualquer incitação a uma tal discriminação, ou quaisquer atos de discriminação com este objetivo, tendo em vista os princípios formulados na Declaração Universal dos Direitos do Homem e os direitos expressamente enumerados no art. V da presente Convenção, *inter alia*:**
>
> **a) a declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio**

existentes no código genético de cada ser humano – que estão na escala dos milhões – não tem maior relação com a sua procedência geográfica ou étnica. No estudo da variabilidade genética humana, verifica-se que de 90 a 95% dela ocorre dentro dos chamados 'grupos raciais', não entre eles. Em síntese, como diz Sérgio Danilo Pena: 'há apenas uma raça do *homo sapiens*: a raça humana'" (pp. 61-62 do parecer, ora juntado aos autos).

raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor, ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento (...)".

Em total consonância com o mandamento internacional, o Brasil editou, logo após a promulgação da Constituição democrática, a **Lei Federal n.º 7.716, de 05 de janeiro de 1989**, que "define os crimes resultantes de preconceitos de raça ou de cor".

O art. 20 do citado diploma infraconstitucional definiu como crime "**praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional**" e previu uma forma qualificada do delito se "cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza".

No caso dos autos, o crime de racismo foi cometido por intermédio do mais poderoso meio de comunicação da atualidade – a **rede mundial de computadores - INTERNET**.

Qualquer pessoa, em qualquer lugar do mundo, desde que conectada à rede, poderá acessar as páginas publicadas pelos investigados. Evidente, portanto, o requisito da transnacionalidade, exigido pelo inciso V, art. 109, da Constituição da República, para justificar a competência desta Justiça Federal.

Ante todo o exposto, pede o Ministério Público Federal, com fundamento nos arts. 240 e ss. do Código de Processo Penal, a expedição do competente mandado judicial para a busca e apreensão de todos os **computadores** instalados nos dois endereços desta subseção judiciária referidos nesta petição, quais sejam, **Rua XXXXXX, 21 – Itaim Bibi** e **Rua XXXXXXXX, 86 – Jardim Hípico**. Pede, também, a **autorização judicial para busca e apreensão de objetos (inclusive CD's e disquetes) e documentos que possuam conteúdo discriminatório ou que auxiliem na apuração da participação de outras pessoas no delito aqui investigado**.

Pede, ainda, desde logo, **autorização judicial para o acesso aos dados contidos nos computadores, disquetes e CD's que venham a ser apreendidos nos dois endereços**.

Termos em que,
P. Deferimento.

São Paulo, 29 de setembro de 2003.

2. <u>Pedido de interceptação do fluxo de dados telemáticos. Pornografia infantil</u>.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO.

*O **<u>MINISTÉRIO PÚBLICO FEDERAL</u>**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência expor e requerer o seguinte:*

O presente procedimento de investigação foi instaurado para apurar *notitia criminis* enviada por *e-mail* a esta Procuradoria da República. Nela constava informação de que o *site* www.xxxxxxx.com.br estaria veiculando material pedófilo.

O *site* seria, em princípio, destinado à divulgação de contos eróticos. Entretanto, pesquisa realizada na seção "incesto" revelou que alguns usuários utilizam o *site* para solicitar e oferecer imagens pornográficas de crianças e adolescentes .

Um dos usuários, cujo e-mail é zzzzzzz@bol.com.br, postou a seguinte mensagem:

> "Título: Garotinha taradinha
>
> Oi, me chamo Samuel, gosto de brincar com <u>menininhas de 5,6,7,8,9 e 10 aninhos.</u> Se você quer trocar fotos de garotinhas me mande que mandarei também para você...
>
> <u>Mas lembre-se só de garotinhas novinhas.</u>"
>
> Numa outra mensagem, o mesmo usuário revela:
>
> "Título: Garotinhas novinhas
>
> (...) Favor se você tiver fotos reais de garotinhas inocentes me envie que enviarei também de volta pra você uma foto que tirei em casa com a filhinha da minha vizinha de <u>6 aninhos</u>, ela xxxxxxx e eu xxxxxxxxxxx."

O usuário do *e-mail* xxxxxxxx@bol.com.br, por sua vez postou a seguinte mensagem:

> "Título: quer vc. ninfetas!!!
>
> Quero xxxxxx c/ ninfetas pois sou louco por ninfetinhas. Peço sigilo e discrição. (entre 11 a 13 anos). aguardo ansioso"

No caso dos autos, os crimes acima indicados estão sendo cometidos por intermédio do mais poderoso meio de comunicação da atualidade – a **rede mundial de computadores - INTERNET**.

A competência para a autorização da interceptação do fluxo e a quebra do sigilo de dados telemáticos, adiante requerida, pertence à Justiça Federal, nos termos do disposto no art. 109, inciso V, da Constituição da República (*in verbis*: "aos juízes federais compete processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente").

Evidente, aqui, o requisito da transnacionalidade, exigido pelo inciso V, art. 109, da Constituição da República, para justificar a competência desta Justiça Federal, vez que em qualquer lugar do mundo pode-se acessar as mensagens postadas.

É indispensável, para o prosseguimento das investigações, a identificação dos autores das mensagens e, mais ainda, é necessário verificar o que esses usuários veiculam em suas contas de e-mail, para saber se enviam e recebem imagens pornográficas de crianças e adolescentes. Numa fase posterior, poderá se apurar, também, os possíveis crimes de estupro e atentado violento ao pudor, sugeridos em algumas das mensagens postadas.

Há nos autos, Excelência, indícios razoáveis da materialidade e da autoria do delito tipificado no artigo 241 da Lei 8.069/90, o qual é apenado com reclusão de 2 a 6 anos e multa. Ademais, a interceptação do fluxo telemático e a quebra do sigilo dos dados telemáticos, como exposto acima, é o único meio possível pelo qual pode ser feita a prova. Os usuários de Internet se beneficiam da Internet, face à dificuldade de investigação de crimes dessa natureza e, contando com a impunidade, continuando praticando seus crimes.

Os *e-mails* xxxxxx@bol.com.br e xxxxxxx@bol.com.br são os únicos cujo provedor encontra-se no Brasil e optou-se, por esse motivo, requerer primeiramente o acesso aos dados desses usuários.

O provedor dos dois e-mails é o Universo Online, sediado em São Paulo, na Av. Brigadeiro Faria Lima, 1384 – 10º andar. Todos os demais endereços eletrônicos possuem provedor estrangeiro, mesmo os que terminam em "br".

Por todo o exposto, o Ministério Público Federal requer, quanto aos usuários dos endereços eletrônicos xxxxxxxxxx@bol.com.br e xxxxxxxxx@bol.com.br:

(i) a imediata **INTERCEPTAÇÃO DO FLUXO DE DADOS TELEMÁTICOS**, nos termos do artigo 1º, parágrafo único, da Lei 9.296/96, pelo prazo de quinze dias, devendo o provedor de acesso UOL remeter ao Ministério Público Federal , em tempo real, e, posteriormente, também em papel, cópia de todos os *e-mails* recebidos e enviados pelos usuários, bem como dos arquivos neles anexados. A cópia em tempo real deverá ser

encaminhada por meio de “conta-espelho” (conta criada pelo provedor com usuário e senha, réplica da conta original); e

(ii)a **QUEBRA DO SIGILO DE DADOS TELEMÁTICOS**, devendo a empresa UOL apresentar, no prazo de cinco dias, todos os dados dos assinantes das mencionadas contas de *e*-mail, inclusive as datas de acesso e respectivos IPs e *e-mails* eventualmente armazenados.

Com o objetivo de assegurar o prosseguimento das investigações, requer o Ministério Público Federal a **DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS**.

Para o mesmo fim, requer que no ofício expedido à empresa STS conste ordem expressa para a **preservação do sigilo da ordem judicial ora requerida**.

São Paulo, 04 de outubro de 2004.

3. <u>Pedido de quebra de sigilo de dados telemáticos para provedor que hospeda *site*.</u> Pornografia infantil.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO.

Procedimento Criminal n.º XXXXXXXX

O **<u>MINISTÉRIO PÚBLICO FEDERAL</u>**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência expor e requerer o seguinte:

O presente procedimento de investigação foi instaurado para apurar veiculação de imagens pornográficas envolvendo crianças e adolescentes por usuários da Rede Mundial de Computadores, em virtude de *noticia criminis* enviada por e-mail a esta Procuradoria.

Consta da notícia que o site www.ubbi.com.br hospeda páginas com imagens pornográficas de crianças e adolescentes. De fato, a pesquisa em referido site demonstrou existirem "álbuns" contendo imagens pornográficas de crianças e adolescentes, conforme cópias ora anexadas.

Estando presentes indícios razoáveis da materialidade e da autoria do delito tipificado no artigo 241 da Lei 8.069/90, e sendo a quebra do sigilo dos dados telemáticos o único meio possível pelo qual pode ser feita a prova, requeiro a QUEBRA DO SIGILO DE DADOS TELEMÁTICOS, devendo a empresa UBBI[16] apresentar, <u>no prazo de quinze dias</u>, cópias em CD-R das páginas anexas, todos os dados cadastrados do autor do "álbuns" e, ainda, dos logs e IPs gerados no momento da transmissão.

São Paulo, 18 de janeiro de 2005.

[16] Endereço: Rua XXXXX – São Paulo-SP, conforme pesquisa anexa.

4. <u>Pedido de quebra de sigilo de dados telemáticos para concessionária de telefonia. Pornografia infantil</u>.

3ª Vara Federal Criminal da Subseção Judiciária de São Paulo

Autos n.º XXXXXXXXX

MM. Juiz:

1. Ciente da decisão prolatada às fls. 59/61.

2. Analisando-se os documentos fornecidos pelo provedor Yahoo!, juntados às fls. 45/58, verificou-se, em primeiro lugar, através dos dados cadastrais fornecidos pelo usuário do e-mail xxxxxxxxxx@yahoo.com.br (fls. 45), que o IP utilizado por ele no momento da criação da conta foi o 200.171.135.82.

Em pesquisa realizada junto ao site *registro.br*, constatou-se que o IP em questão está registrado na empresa TELECOMUNICACOES DE SAO PAULO S.A. – TELESP, sendo, portanto, este o provedor que fornece acesso à internet para o usuário.

Diante do exposto, havendo indícios razoáveis da prática de crime gravíssimo – publicação, por meio da rede mundial de computadores, de fotografias e imagens com pornografia e cenas de sexo explícito envolvendo crianças e adolescentes – requer o Ministério Público Federal a **QUEBRA DE SIGILO DE DADOS TELEMÁTICOS**, devendo a concessionária TELESP (Rua Martiniano de Carvalho, n.º 851, São Paulo/SP) informar, no prazo de 05 (cinco) dias, os dados cadastrais do usuário que se conectou à internet no dia 09 de fevereiro de 2.002, às 19h50m06s (BRST GMT – 0200) e às 16h32m09s (EST GMT – 0500), utilizando-se do IP 200.171.135.82, em ambos os horários;

São Paulo, 16 de março de 2005.

5. <u>Quesitos para exame pericial em computadores apreendidos. Pornografia infantil</u>.

1ª Vara Criminal Federal da Seção Judiciária de São Paulo - SP

Autos n.º XXXXXXXX

MM. Juiz Federal:

Trata-se de inquérito policial instaurado com o objetivo de apurar prática do crime previsto no artigo 241 da Lei 8.069/90.

Da busca e apreensão realizada em três endereços apurados a partir de e-mails envolvidos em pedofilia, resultou vasto material que deverá ser encaminhado à perícia. Passo, então a formular os QUESITOS que deverão ser respondidos pela perícia:

1) Há *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* no material apreendido? Qual sua natureza (filmes, fotos, etc)?

2) É possível afirmar que houve divulgação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* desses computadores para outros usuários da Rede Mundial? Qual o material enviado? Para quem esse material foi enviado?

3) Há mensagens recebidas de outros usuários da Internet que contenham *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente*? Quais os endereços eletrônicos dos remetentes? Qual o material recebido?

4) Quais páginas da Internet foram acessadas pelos usuários do material apreendido?

5) É possível afirmar que os usuários participavam de grupos de discussão e/ou comunidades em que se divulgavam ou publicam *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente*? Quais são?

6) Os usuários possuem outra contas de e-mail cadastradas? Quais são?

7) É possível recuperar arquivos ou mensagens eletrônicas apagadas dos computadores? Em caso afirmativo, há arquivos ou mensagens recuperadas em que haja publicação ou divulgação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

8) Há elementos que permitam concluir que *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* foram produzidas ou editadas através dos comutadores apreendidos?

9)Existem aplicativos de edição e vídeos instalados nos computadores?

10) É possível afirmar que os usuários obtiveram para si ou para outrem vantagem patrimonial com a divulgação ou publicação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

11) Houve vendas de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

12) Há outras informações úteis para a elucidação do caso?

São Paulo, 21 de setembro de 2004.

6. <u>Denúncia. Art. 241 do ECA</u>.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA 1ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO.

Autos n.º VVVVVVVVVVV

O **<u>MINISTÉRIO PÚBLICO FEDERAL</u>**, pelo Procurador da República que esta subscreve, vem respeitosamente à presença de Vossa Excelência, oferecer a presente

DENÚNCIA

em face de **<u>XXXXXXXXXX</u>**, brasileiro, solteiro, advogado, portador da cédula de identidade RG 00000000000 SSP/SP, inscrito na OAB/SP sob o número 000000, nascido em 22 de abril de 1972 em São Paulo – SP, filho de XXXXXXX e de XXXXXXX, residente e domiciliado nesta capital na Rua TTTTTT; pela prática da conduta criminosa descrita a seguir:

Consta dos inclusos autos de inquérito policial que o ora denunciado, usuário do e-mail <u>xxxxxxxx@hotmail.com</u>, no dia 31 de Maio de 2.001, às 23h43min06seg, nesta cidade e subseção judiciária, **publicou**, na rede mundial de computadores (*internet*), remetendo ao usuário do e-mail <u>yyyyyy@aol.com</u>, um arquivo denominado "frag08_505.m1v", o qual continha um vídeo com **cena de sexo explícito e pornográfica envolvendo crianças.**

Consta, ainda, que o ora denunciado, usuário do e-mail <u>xxxxxxx@hotmail.com</u>, no dia 31 de Maio de 2.001, às 23h46min21seg, nesta cidade e subseção judiciária, **publicou**, na rede mundial de computadores (*internet*), remetendo ao usuário do e-mail zzzzzz@aol.com, um arquivo denominado "frag08_505.m1v", o qual continha um vídeo com **cena de sexo explícito e pornográfica envolvendo crianças.**

Segundo se apurou, a Divisão de Justiça Criminal do Departamento de Segurança Pública e Lei do Estado de Nova Jersey, nos Estados Unidos da América, noticiou à Superintendência Regional do Departamento de Polícia Federal, no Estado do Rio Grande do Sul, a prática da veiculação de exploração sexual infantil através de imagens divulgadas para todo o mundo pela Internet, detectadas em "site" sediado naquele país, sendo parte dessas imagens oriundas do Brasil (fls. 03/04).

Imagens coletadas no site em questão (www.uuuuuuu.net) foram juntadas aos autos, constando das fls. 14/31. Nelas se verifica claramente o conteúdo pornográfico, no qual aparecem crianças em cenas de sexo.

Conforme se verificou às fls. 09/13, um dos usuários provenientes do Brasil e que estaria participando desse site foi identificado pelo IP 200.183.97.81 e pelo e-mail xxxxxxxxxxx@hotmail.com.

Em decisão de fls. 39/40, a MM. Juíza da 2ª Vara Criminal Federal determinou a quebra do sigilo das comunicações de dados do e-mail acima referido, no sentido de se obter, junto ao provedor de acesso à Internet "Hotmail.com", os dados cadastrais do seu assinante. E também foi determinada a intimação da empresa GLOBOCABO S/A, para que fornecesse os dados do usuário do IP supracitado.

Em resposta, juntada às fls. 44, a "NET São Paulo" informou que o usuário do IP em questão tratava-se do ora denunciado, ou seja, XXXXXXXXX. Foi, ainda, fornecido o endereço do local onde ele realizava os acessos ao site supramencionado.

Em decisão de fls. 54, foi determinada a realização de diligência junto ao endereço obtido, a fim de que fossem confirmadas as informações. Esta foi realizada com êxito, conforme relatório acostado às fls. 67, no qual os agentes federais informaram que no endereço realmente residia a pessoa do ora denunciado.

Diante disso, foi deferida, pela MM. Juíza Federal da 2ª Vara Criminal Federal, a realização de busca domiciliar no endereço em questão, a fim de apreender computadores, fitas de vídeo, fotografias, disquetes, CD-ROMs, revistas e outros elementos que levassem à convicção sobre a prática de crime de pedofilia por parte do ora denunciado.

Dando cumprimento ao mandado judicial, foram apreendidos os objetos descritos às fls. 82/83, os quais se encontravam em poder do ora denunciado. Entre eles, havia um equipamento eletrônico, marca "Toshiba", modelo Libretto 70 CT e uma CPU, completa, além de vários disquetes de 1.44Mb e CR Roms.

O ora denunciado confessou, às fls. 86, que era responsável, à época dos fatos, pelo e-mail xxxxxx@hotmail.com, referido acima. Disse, ainda, que recebe e-mails contendo imagens de adolescentes em cenas de sexo ou pornográficas, sendo que costuma enviar as mensagens pornográficas que recebe a cerca de vinte amigos.

Quanto ao computador e o notebook apreendidos, seus respectivos discos rígidos foram submetidos a exame em mídia de armazenamento computacional, cujo laudo encontra-se às fls. 117/126 dos presentes autos.

No exame feito no disco rígido do computador, verificou-se que ele apresentava indícios de que fora formatado em momento recente à elaboração do laudo, no entanto, logrou-se recuperar arquivos que

haviam sido apagados e que continham imagens pornográficas envolvendo crianças e adolescentes.

Os peritos da Polícia Federal gravaram o material relevante encontrado no computador e no notebook do ora denunciado em três CD-Roms, os quais encontram-se juntados nos presentes autos. Nestes CDs, há milhares de arquivos fotográficos e de vídeos, nos quais crianças com pouca idade e também adolescentes praticam sexo ou tiram a roupa e permanecem em posições degradantes.

No arquivo "frag08_505.m1v", objeto do crime em questão, há um vídeo, no qual duas crianças do sexo masculino encontram-se praticando sexo oral, conforme se verifica num dos CDs acostados aos autos.

Verifica-se, ainda, que há várias mensagens encaminhadas pelo ora denunciado, nas quais ele se utiliza do idioma inglês para manter contato com outros pedófilos, a fim de combinar maneiras de obter novos arquivos contendo material pornográfico infantil. Um exemplo disso é a mensagem encaminhada no dia 31 de maio de 2001, por volta das 19h25min, na qual XXXXXXXXX questiona o seu interlocutor sobre a obtenção de "coisas" naquele dia. Além disso, em outra mensagem, o denunciado explica a um indivíduo como seria possível a troca de filmes e imagens através de ICQ (I Seek You), conforme atesta o laudo às fls. 122.

Se não bastasse esse conteúdo, verificou-se no disco rígido do notebook apreendido que existem diversos arquivos que evidenciam que o usuário possuía cadastro em diversos sítios na Internet de acesso restrito com conteúdo pedófilo. Diversos desses sítios são localizados na Rússia.(fls. 122).

Diante de todo exposto, estando configurada a materialidade do delito e indícios suficientes de sua autoria, **DENUNCIO XXXXXXXXX**, como incurso, por duas vezes, nas penas do art. 241 da Lei n.º 8.069/90, na forma do disposto no artigo 71 do Código Penal, requerendo que, recebida e autuada esta, seja instaurado o competente processo penal, citando e intimando o réu para todos os seus atos, até final condenação, nos termos dos arts. 394 a 405 e 498 a 502 do Código de Processo Penal.

São Paulo, 28 de fevereiro de 2005.

ANEXO III:
ENDEREÇOS ÚTEIS

1. Provedores (de acesso, conteúdo, e-mail etc.).

RAZÃO SOCIAL	RESPONSÁVEL	ENDEREÇO	TELEFONE
AOL Brasil – (América OnLine)	Edson Costamilan Pavão	Av. Industrial, 600 – Centro Industrial – Shopping ABC Plaza - 2º andar – São Paulo – SP – CEP 09080-500	(11) 2191-5900
Click 21 – Comércio de Publicidade Ltda. (Embratel)	Eduardo Vianna Barreto	R. Regente Feijó, 166, 14º andar – Centro - Rio de Janeiro - RJ - CEP 20060-060	(21) 4004 2121
TV Globo Ltda. **(Globo.Com)**		Av. das Américas, 700 - Bloco 2A – Barra da Tijuca - Rio de Janeiro - RJ - CEP 22640-100	(21) 4003-8000/ 8003
Google Brasil (G-Mail e Orkut)	Alexandre Hohagen	Av. Brig. Faria Lima, 3729 – 5º andar – São Paulo – SP – CEP 04538-133	(11) 3443-6333
Internet Group do Brasil Ltda. **(IG)**	Cássio Roberto Urbani Ribas	Rua Amauri, 299 – 7º andar – Jd. Europa – São Paulo – SP – CEP 01448-901	(11) 3065-9901/9999
Microsoft do Brasil (**Hotmail** e **Messenger**)	Karine Yamassaki (Depto. Jurídico)	Av. das Nações Unidas, 12901 - 27º andar - Torre Norte - São Paulo - SP CEP 04578-000	(11) 5504-2155
Terra Networks Brasil S.A.	Carlos Henrique Severo	Av. das Nações Unidas, 12901 – 12º andar – Torre Norte – São Paulo – SP – CEP 04578-000	(11) 5509 0644
UOL – Universo OnLine	Victor Fernando Ribeiro	Av. Brig. Faria Lima, 1384 – 6º andar – São Paulo – SP – CEP 01451-001	(11) 3038-8431
Yahoo do Brasil Internet Ltda.	Regina Lima	R. Fidêncio Ramos, 195 – 12º andar – São Paulo – SP – cep 04551-010	(11) 3054-5200

2. Concessionárias de telefonia fixa no Brasil.

SIGLA	RAZÃO SOCIAL	ENDEREÇO
TELEMAR/RJ	Telemar Norte Leste S.A.	Rua Gal. Polidoro, 99 – Botafogo – Rio de Janeiro – RJ – CEP 22280-001
TELEMAR/MG	Telemar Norte Leste S.A.	Av. Afonso Pena, 4001 – 1º andar – Belo Horizonte – MG – CEP 30130-008
CTBC TELECOM	Cia. de Telecomunicações do Brasil Central	Av. Afonso Pena, 3928 – Bairro Brasil – Uberlândia – MG – CEP 38400-710
TELEMAR/ES	Telemar Norte Leste S.A.	Av. Afonso Pena, 4001 – 1º andar – Belo Horizonte – MG – CEP 30130-008
TELEMAR/BA	Telemar Norte Leste S.A.	Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900
TELEMAR/SE	Telemar Norte Leste S.A.	Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900
TELEMAR/AL	Telemar Norte Leste S.A.	Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900
TELEMAR/PE	Telemar Norte Leste S.A.	Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900
TELEMAR/PB	Telemar Norte Leste S.A.	Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900
TELEMAR/RN	Telemar Norte Leste S.A.	Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900
TELEMAR/CE	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/PI	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/MA	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/PA	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/AP	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/AM	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
TELEMAR/RR	Telemar Norte Leste S.A.	Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510
BRASIL TELECOM/SC	Brasil Telecom S.A.	Av. Madre Benvenuta, 2080 – Itacorubi – Florianópolis – SC – CEP 88035-900
BRASIL TELECOM/PR	Brasil Telecom S.A.	Av. Manoel Ribas, 115 – Curitiba – PR – CEP 80510-900
SERCOMTEL	Sercomtel S.A. Telecomunicações	R. Prof. João Cândido, 555 – Centro – Londrina – PR – CEP 86010-000
BRASIL TELECOM/MS	Brasil Telecom S.A.	R. Tapajós, 660 – Vila Rica – Campo Grande – MS – CEP 79022-210
BRASIL TELECOM/MT	Brasil Telecom S.A.	R. Barão do Melgaço, 3209 – Centro Sul – Cuiabá – MT – CEP 78020-902

BRASIL TELECOM/GO-TO	Brasil Telecom S.A.	BR 153, km. 06 – CAEL – V. Redenção – Goiânia – GO – CEP 74845-090
BRASIL TELECOM/DF	Brasil Telecom S.A.	SCS Quadra 02 - Bloco E – Ed. Telebrasília – Brasília – DF – CEP 70390-025
BRASIL TELECOM/RO-AC	Brasil Telecom S.A.	Av. Lauro Sodré, 3290 – Bairro dos Tanques – Porto Velho – RO – CEP 78903-711
BRASIL TELECOM/Pelotas	Brasil Telecom S.A.	Av. Borges de Medeiros, 512 – Porto Alegre – RS – CEP 90020-022
BRASIL TELECOM/RS	Brasil Telecom S.A.	Av. Borges de Medeiros, 512 – Porto Alegre – RS – CEP 90020-022
BRASIL TELECOM/Matriz	Brasil Telecom S.A.	SAI SUL – ASP Lote D – Brasília – DF – CEP 71215-000
TELESP	Telecomunicações de São Paulo S.A.	Rua Martiniano de Carvalho, 851 – 20º e 21º andar – São Paulo – SP – CEP 01321-002

3. ABRANET e Comitê Gestor da Internet.

NOME	CONTATO	ENDEREÇO	TELEFONE
Comitê Gestor da Internet no Brasil – CGI	Demi Getschko e Hartmut Richard Glaser	Avenida das Nações Unidas, 11541 - 7º andar – São Paulo – SP - CEP 04578-000	(11) 5509 3503/3513
ABRANET - Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet	António Alberto Valente Tavares	R. Tabapuã, 627 - 3º andar - sala 34 – CEP 04533-012	(11) 3078-3866

ANEXO IV:
ACORDOS CELEBRADOS PELA PR-SP

1. Termo de compromisso de integração operacional celebrado com principais provedores de acesso de São Paulo.

Pelo presente instrumento,

A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO, órgão integrante do Ministério Público Federal, sediada nesta capital, na Rua Peixoto Gomide, 768 – Cerqueira César, neste ato representada pela Excelentíssima Senhora Procuradora Chefe, Dra. ADRIANA ZAWADA MELO e pelos Procuradores Regionais dos Direitos do Cidadão, Dr. SERGIO GARDENGHI SUIAMA e Dra. ADRIANA DA SILVA FERNANDES;

Os provedores de acesso à internet UNIVERSO ON LINE, sediado na Avenida Brigadeiro Faria Lima, 1384 - 6º andar, neste ato representado pelo Ilustríssimo Senhor VICTOR FERNANDO RIBEIRO, RG 29.089.911-4 SSP/SP; INTERNET GROUP DO BRASIL LTDA. - IG, sediado na Rua Amauri, nº 299 - 7º andar, neste ato representado pelo Ilustríssimo Senhor CÁSSIO ROBERTO URBANI RIBAS - OAB/SP nº 154.045; TERRA NETWORKS BRASIL S.A., na Av. Nações Unidas, 12.901, 12º andar, Torre Norte, neste ato representado pelo Ilustríssimo Senhor CARLOS HENRIQUE SEVERO, RG nº 39590691-X; AOL BRASIL, sediado na Av. Industrial, 600 - Centro Empresarial ABC Plaza, 2º andar, neste ato representado pelo Ilustríssimo Senhor EDSON COSTAMILAN PAVÃO, OAB/SP nº 151.079; CLICK 21 COMÉRCIO DE PUBLICIDADE LTDA., sediado na Rua Rejente Feijó, 166, 14 andar, Centro, Rio de Janeiro – RJ, neste ato representado pelo Ilustríssimo Senhor EDUARDO VIANNA BARRETO, RG nº 066.078.12-2 IFP/RJ;

A ASSOCIAÇÃO BRASILEIRA DOS PROVEDORES DE ACESSO, SERVIÇOS E INFORMAÇÕES DA REDE INTERNET - ABRANET, sediada nesta capital, na Rua Tabapuã, 697 - 3° andar, neste ato representada por seu Presidente, o Ilustríssimo Senhor ANTÔNIO ALBERTO VALENTE TAVARES;

As EMPRESAS DE SERVIÇOS DE INTERNET ASSOCIADAS À ABRANET SIGNATÁRIAS do presente termo;

O COMITÊ GESTOR DA INTERNET NO BRASIL, sediada na Avenida das Nações Unidas, 11541, 7º andar, neste ato representado pelo Ilustríssimo Senhor DEMI GETSCHKO, RG nº 5.490.048-7; têm justo e acertado o seguinte:

CONSIDERANDO que o art. 227 da Constituição da República estabelece ser dever da família, da sociedade e do Estado colocar as crianças e os adolescentes a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão; e que o parágrafo 4º do mesmo artigo obriga o Estado a punir severamente o abuso, a violência e a exploração sexual da criança e do adolescente;

CONSIDERANDO que o art. 34 da Convenção das Nações Unidas sobre os Direitos da Criança, ratificada pelo Brasil, obriga os Estados-partes a proteger a criança contra todas as formas de exploração e abuso sexual, inclusive no que se refere à exploração da criança em espetáculos ou materiais pornográficos;

CONSIDERANDO que a Conferência Internacional sobre o Combate à Pornografia Infantil na Internet (Viena, 1999) demanda a criminalização, em todo o mundo, da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil, e enfatiza a importância de cooperação e parceria mais estreita entre governos e a indústria da Internet;

CONSIDERANDO que o art. 5º do Estatuto da Criança e do Adolescente (Lei Federal n.º 8.069/90) dispõe que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais;

CONSIDERANDO que o art. 70 do mesmo Estatuto determina ser dever de todos prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente;

CONSIDERANDO que, nos termos do art. 201, inciso VIII, do Estatuto da Criança e do Adolescente, compete ao Ministério Público zelar pelo efetivo respeito aos direitos e garantias legais assegurados às crianças e adolescentes, promovendo as medidas judiciais e extrajudiciais cabíveis;

CONSIDERANDO que a Lei Federal n.º 10.764/03 alterou a redação do art. 241 do Estatuto da Criança e do Adolescente para incluir a responsabilização criminal de quem assegura o acesso à rede mundial de computadores ou os meios ou serviços para o armazenamento das fotografias, cenas ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente;

CONSIDERANDO que a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, promulgada pela Assembléia Geral das Nações Unidas em 21 de dezembro de 1965, e ratificada pelo Brasil em 27 de março de 1968, obriga os Estados-partes a declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra

qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento;

CONSIDERANDO que a mesma Convenção obriga os Estados-partes a tomar todas as medidas apropriadas para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupos ou organizações;

CONSIDERANDO que é objetivo da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, idade e quaisquer outras formas de discriminação (CR, art. 3º, IV);

CONSIDERANDO, ainda, que o art. 5º, inciso XLI, da Constituição da República ordena a punição de qualquer discriminação atentatória dos direitos e liberdades fundamentais;

CONSIDERANDO que a Lei Federal n.º 7.716, de 05 de janeiro de 1989, tipifica o delito de "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" e qualifica a conduta quando cometida por intermédio dos meios de comunicação social ou publicação de qualquer natureza (art. 20, caput, e § 3º);

CONSIDERANDO que o Plano Nacional de Direitos Humanos (PNDH) ordena a edição de medidas que busquem coibir o uso da Internet para incentivar práticas de violação dos direitos humanos;

CONSIDERANDO a competência da Justiça Federal para processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (CR, art. 109, inciso V);

CONSIDERANDO que a Organização Não-Governamental italiana "*Rainbow Phone*", em seu relatório anual publicado na Internet, apontou o Brasil como o quarto país no mundo em número de sítios de pornografia infantil;

CONSIDERANDO, o grande número de denúncias de sítios brasileiros com conteúdo racista e discriminatório, o que está a exigir providências interinstitucionais, em decorrência dos bens jurídicos fundamentais atacados, quais sejam, a dignidade da pessoa humana, a cidadania e a igualdade fundamental entre todas as pessoas;

CONSIDERANDO, finalmente, a necessidade de integrar as partes signatárias na aplicação dos dispositivos constitucionais e legais acima referidos;

RESOLVEM celebrar o presente Termo de Compromisso de Integração Operacional com a finalidade de unir esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação,

instrumentalizadas via Internet. Para tal, ficam acordadas as seguintes CLÁUSULAS:

Cláusula Primeira: Ficam o Ministério Público Federal e a Polícia Federal comprometidos a manter sítio na Internet de enfrentamento à pornografia infantil, ao racismo e a outras formas de discriminação, informando o público acerca da legislação aplicável e facultando ao usuário formular notícia de crimes cibernéticos cuja repressão esteja no âmbito da repressão do Estado brasileiro.

Cláusula Segunda: Ficam os provedores de serviço de Internet signatários comprometidos a:

a) manter, permanentemente, em suas páginas, selo institucional de campanha governamental contra a pornografia infantil e contra a veiculação de preconceitos quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação;

b) fazer, periodicamente, chamadas contra essas práticas, através de quaisquer meios de que dispõem para a comunicação regular com seus usuários, tais como documentos de cobrança, *e-mails* e instrumentos contratuais;

c) orientar o público sobre a utilização não criminosa de salas de bate-papo, grupos e fóruns de discussão, *blogs*, páginas pessoais e outros serviços disponibilizados ao usuário;

d) inserir, nos contratos de adesão ao serviço de acesso que venham a ser assinados a partir da vigência deste termo, cláusula que preveja a rescisão da relação jurídica na hipótese do usuário valer-se do provedor para veicular fotografias e imagens de pornografia infantil, ou idéias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação;

e) manter *link* para o sítio previsto na cláusula primeira;

f) manter, sem prejuízo do previsto na alínea anterior, *link* pelo qual os usuários possam noticiar ao provedor signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum eletrônico, ou outro serviço prestado pelo próprio provedor;

g) informar imediatamente ao Ministério Público Federal, por via eletrônica ou outros meios de comunicação, tão logo tomem conhecimento de que abrigam pornografia infantil ou conteúdo manifestamente discriminatório em razão da origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação, ou ainda de que usuários do provedor estão usando o acesso à rede para praticar os crimes tipificados no art. 241 da Lei Federal n.º 8.069/90 e no art. 20 da Lei Federal n.º 7.716/89, assegurada a proteção ao sigilo dos dados telemáticos;

h) preservar e armazenar, pelo prazo mínimo de 6 (seis) meses ou prazo superior que venha a ser estabelecido pela legislação, o registro de *logs* de acesso discado e, quando possível, também os IPs originários dos usuários dos serviços de *web page*, salas de bate-papo, *fotologs*, fóruns de discussão *on-line* e outros. O disposto nesta cláusula aplicar-se-á mesmo após o prazo mínimo indicado, se houver solicitação escrita da Polícia Federal ou do Ministério Público Federal, até que estas instituições providenciem a competente ordem judicial de quebra de sigilo de dados telemáticos;

j) solicitar e manter os dados cadastrais informados por seus assinantes de acesso;

l) exigir que os novos usuários do serviço de acesso informem o número de algum documento validável de identificação, como por exemplo o número do RG ou do CPF;

Cláusula Terceira: As obrigações assumidas no presente Termo permanecerão válidas e obrigam as empresas associadas à ABRANET, signatárias deste Termo, ainda que deixem de ser associadas à Associação signatária.

Cláusula Quarta: O presente termo vigorará por tempo indeterminado e está aberto à adesão de outros provedores que concordem integralmente com seus termos.

Cláusula Quinta: O presente termo entrará em vigor após 60 (sessenta) dias de sua assinatura.

São Paulo, 10 de novembro de 2005.

2. Termo de cooperação celebrado com o hotline Safernet Brasil.

Pelo presente instrumento,

A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO, órgão do Ministério Público Federal sediado nesta capital, na Rua Peixoto Gomide, 768 – Cerqueira César, neste ato representada pela Excelentíssima Senhora Procuradora Chefe em exercício, Dra. Thaméa Danelon Valiengo e pelo Procurador Regional dos Direitos do Cidadão, Dr. SERGIO GARDENGHI SUIAMA e a

SAFERNET BRASIL, associação civil de direito privado sem fins lucrativos e econômicos, de atuação nacional, de duração ilimitada e ilimitado número de membros, sem vinculação político partidária, inscrita no CNPJ/MF sob o número 07.837.984/0001-09, com sede provisória na cidade de Salvador, Estado da Bahia, na Avenida Tancredo Neves 1632, Torre Norte, sala 2101 - Caminho das Árvores, neste ato representada por seu Presidente, Dr. THIAGO TAVARES NUNES DE OLIVEIRA,

CONSIDERANDO que o art. 227 da Constituição da República estabelece ser dever da família, da sociedade e do Estado colocar as crianças e os adolescentes a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão; e que o parágrafo 4º do mesmo artigo obriga o Estado a punir severamente o abuso, a violência e a exploração sexual da criança e do adolescente;

CONSIDERANDO que o art. 34 da Convenção das Nações Unidas sobre os Direitos da Criança, ratificada pelo Brasil, obriga os Estados-partes a proteger a criança contra todas as formas de exploração e abuso sexual, inclusive no que se refere à exploração da criança em espetáculos ou materiais pornográficos;

CONSIDERANDO que o art. 5º do Estatuto da Criança e do Adolescente (Lei Federal n.º 8.069/90) dispõe que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais;

CONSIDERANDO que, nos termos do art. 201, inciso VIII, do Estatuto da Criança e do Adolescente, compete ao Ministério Público zelar pelo efetivo respeito aos direitos e garantias legais assegurados às crianças e adolescentes, promovendo as medidas judiciais e extrajudiciais cabíveis;

CONSIDERANDO que o art. 241 do Estatuto da Criança e do Adolescente tipifica as condutas criminosas de “apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente”;

CONSIDERANDO que a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, promulgada pela Assembléia Geral das Nações Unidas em 21 de dezembro de 1965, e ratificada pelo Brasil em 27 de março de 1968, obriga os Estados-partes a reprimir qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento;

CONSIDERANDO que a mesma Convenção obriga os Estados-partes a tomar todas as medidas apropriadas para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupos ou organizações;

CONSIDERANDO que é objetivo da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, idade e quaisquer outras formas de discriminação (CR, art. 3º, IV);

CONSIDERANDO, ainda, que o art. 5º, inciso XLI, da Constituição da República ordena a punição de qualquer discriminação atentatória dos direitos e liberdades fundamentais;

CONSIDERANDO que a Lei Federal n.º 7.716, de 05 de janeiro de 1989, tipifica o delito de "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" e qualifica a conduta quando cometida por intermédio dos meios de comunicação social ou publicação de qualquer natureza (art. 20, caput, e § 3º);

CONSIDERANDO que o Plano Nacional de Direitos Humanos (PNDH) ordena a edição de medidas que busquem coibir o uso da Internet para incentivar práticas de violação dos direitos humanos;

CONSIDERANDO a competência da Justiça Federal para processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (CR, art. 109, inciso V);

CONSIDERANDO que a Organização Não-Governamental italiana "*Rainbow Phone*", em relatório anual publicado na Internet, apontou o Brasil como o quarto país no mundo em número de sítios de pornografia infantil;

CONSIDERANDO que a Conferência Internacional sobre Combate à Pornografia Infantil na Internet (Viena, 1999) demanda a criminalização, em todo o mundo, da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil, e enfatiza a importância de cooperação e parceria mais estreita entre o governo, a sociedade civil e a indústria da Internet;

CONSIDERANDO o grande número de denúncias de sítios brasileiros com conteúdo racista e discriminatório, o que está a exigir providências interinstitucionais, em decorrência dos bens jurídicos fundamentais atacados, quais sejam, a dignidade da pessoa humana e a igualdade fundamental entre todas as pessoas;

CONSIDERANDO a constituição, no âmbito da Procuradoria da República no Estado de São Paulo, de grupo especializado no combate aos crimes cibernéticos;

CONSIDERANDO a experiência acumulada pelos fundadores da organização-parte na concepção, planejamento, desenvolvimento e operação do projeto “Hotline-Br”;

CONSIDERANDO que a atual dispersão dos canais de denúncia de crimes cibernéticos prejudica, sensivelmente, a persecução penal, favorecendo a impunidade em casos graves de pornografia infantil e crimes de ódio;

CONSIDERANDO, finalmente, a necessidade de integrar as partes signatárias na aplicação dos dispositivos constitucionais e legais acima referidos;

RESOLVEM celebrar o presente TERMO DE MÚTUA COOPERAÇÃO TÉCNICA, CIENTÍFICA E OPERACIONAL com a finalidade de unir esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação, instrumentalizadas via Internet. Para tal, ficam acordadas as seguintes CLÁUSULAS:

CLÁUSULA PRIMEIRA – OBJETO

O presente termo tem por objeto a cooperação técnica, científica e operacional entre as partes celebrantes, com vistas:

a. à centralização do recebimento, processamento, encaminhamento e acompanhamento on-line de notícias de crimes contra os direitos humanos praticados com o uso da rede mundial de computadores – Internet – no Brasil;

b. ao intercâmbio e difusão de tecnologias baseadas em plataformas livres e de código aberto, para serem gratuitamente utilizadas pelas Procuradorias da República nos Estados e no Distrito Federal e também pelas autoridades policiais brasileiras;

c. ao desenvolvimento de projetos e atividades voltadas para o treinamento de recursos humanos, editoração e publicação, planejamento e desenvolvimento institucional abrangendo as áreas de pesquisa e extensão, com o intuito de debater e assegurar a efetiva proteção e promoção dos direitos humanos na sociedade da informação.

Parágrafo único. Para fins do disposto neste termo, a expressão “crimes contra os direitos humanos” compreende os seguintes delitos: a) crimes de ódio tipificados no art. 20 e §§ da Lei Federal n.º 7.716/89; b) crime de pornografia infantil tipificado no art. 241 da Lei Federal n.º 8.069/90; c) crimes contra o sentimento religioso tipificados no art. 208 do Código Penal brasileiro; d) crime de incitação ao genocídio, previsto no art. 3º da Lei Federal n.º 2.889/56; e) apologia ou incitação aos crimes acima indicados ou a outros delitos contra a vida, a integridade física, a liberdade (inclusive sexual) e a incolumidade pública, desde que de competência da Justiça Federal brasileira; e) crime de quadrilha ou bando (art. 288 do Código Penal brasileiro), se conexo aos crimes acima indicados.

CLÁUSULA SEGUNDA – COMPROMISSOS COMUNS

Para a consecução dos objetivos indicados na cláusula primeira, as partes comprometem-se neste ato a:

a. desenvolver, em parceria, estudos e pesquisas buscando criar e aperfeiçoar as tecnologias de enfrentamento aos crimes cibernéticos, disponibilizando o conhecimento gerado para as autoridades brasileiras envolvidas na persecução penal;

b. produzir relatórios e notas técnicas com o objetivo de orientar a atuação das autoridades envolvidas no enfrentamento aos crimes contra os direitos humanos na Internet;

c. promover o intercâmbio de informações, tecnologias, técnicas de rastreamento e assemelhadas, através da organização de cursos, oficinas e outras atividades de capacitação;

d. promover campanhas conjuntas para a conscientização da sociedade em relação à utilização adequada da Internet, visando à proteção e promoção dos direitos humanos na sociedade da informação.

CLÁUSULA TERCEIRA – OBRIGAÇÕES DA SAFERNET BRASIL

A SAFERNET BRASIL compromete-se, neste ato, a:

a. manter portal na Internet para a recepção de notícias de crimes contra os direitos humanos, contendo informações e orientações ao público sobre o uso seguro e lícito da Internet;

b. processar e encaminhar exclusivamente à Procuradoria da República em São Paulo as notícias recebidas, quando o provedor de acesso ou de hospedagem do material criminoso estiver sediado no Estado de

São Paulo, ou quando houver indícios de que o autor do fato delituoso estiver no mesmo Estado;

c. comunicar as demais notícias de fatos criminosos recebidas às autoridades com atribuição para investigá-las, na forma do art. 4º, § 3º, do Código de Processo Penal, ou às Procuradorias da República nos Estados e no Distrito Federal, mediante a celebração de termos de cooperação específicos;

d. fornecer, gratuitamente, os recursos tecnológicos e o treinamento necessários ao pleno desenvolvimento das ações previstas neste termo de cooperação.

§ 1º. A associação signatária declara-se, neste ato, ciente de que o presente ato tem natureza gratuita, e que, portanto, o adimplemento das obrigações contidas neste termo não importará em contraprestação financeira por parte da Procuradoria da República no Estado de São Paulo.

§ 2º. Na medida de suas possibilidades financeiras e jurídicas, a Procuradoria da República no Estado de São Paulo prestará o suporte necessário à execução das obrigações contidas no cláusula anterior e na alínea "d" da presente cláusula.

CLÁUSULA QUARTA – COMPROMISSOS DA PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO

A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO compromete-se, neste ato, a:

a. receber e processar todas as notícias de fatos criminosos encaminhadas pela organização-parte na forma da alínea "b" da cláusula anterior, com o objetivo de comprovar a autoria e a materialidade dos fatos criminosos comunicados;

b. manter, em sua página eletrônica, *banner* contendo os nomes das partes e link para o portal referido na alínea "a" da cláusula anterior;

c. solicitar aos provedores de acesso e às instituições anuentes, signatários do documento "Termo de Compromisso de Integração Operacional" celebrado em 10 de novembro de 2005, que coloquem, em suas páginas, o *link* e o *banner* referidos na alínea anterior, como forma de cumprimento da obrigação assumida na alínea "e" da cláusula segunda do referido documento;

d. noticiar a celebração do presente termo de cooperação à Procuradoria Geral da República, à Procuradoria Federal dos Direitos do Cidadão, às Procuradorias da República nos Estados e no Distrito Federal, ao Departamento de Polícia Federal e à Secretaria Especial dos Direitos

Humanos da Presidência da República, e sugerir a esses e a outros órgãos afins que mantenham em suas páginas eletrônicas o *banner* e o *link* indicados na alínea “b” desta cláusula, com o objetivo de centralizar as notícias de crimes cibernéticos contra os direitos humanos em um único canal de denúncias.

CLÁUSULA QUINTA - SIGILO

As partes se obrigam a manter sob o mais estrito sigilo os dados e informações referentes aos projetos e ações consideradas e definidas como confidenciais, não podendo de qualquer forma, direta ou indiretamente, dar conhecimento, a terceiros não autorizados, das informações confidenciais trocadas entre os acordantes ou por eles geradas na vigência do presente termo.

CLÁUSULA SEXTA – CASOS OMISSOS:

Os casos omissos no presente ajuste serão resolvidos de comum acordo entre as partes, podendo ser firmados, se necessário, Termos Aditivos que farão parte integrante deste instrumento.

CLÁUSULA SÉTIMA - ALTERAÇÃO E DENÚNCIA

O presente instrumento poderá ser alterado em qualquer de suas cláusulas, mediante Termo Aditivo, bem como denunciado, independentemente de prévia notificação, no caso de inadimplemento das obrigações assumidas, ou por conveniência das partes, mediante notificação com antecedência de 30 (trinta) dias.

CLÁUSULA OITAVA – VIGÊNCIA

O presente termo vigorará por tempo indeterminado, facultado às partes o exercício, a qualquer tempo, do direito potestativo referido na cláusula anterior.

E por estarem justos e acordados, assinam o presente CONVËNIO DE COOPERAÇÃO TÉCNICA, CIENTÍFICA E OPERACIONAL em 03 (três) vias de igual teor e forma, na presença das testemunhas signatárias, para que se produzam os necessários efeitos jurídicos e legais.

São Paulo, 29 de março de 2006.

ANEXO V:
CONVENÇÃO SOBRE A CIBERCRIMINALIDADE
(ORIGINAL EM INGLÊS)

Observação: a Convenção sobre a Criminalidade Cibernética foi adotada pelo Conselho da Europa em 23 de novembro de 2001. É aberta à assinatura de países que não integram o Conselho (Canadá, Japão, África do Sul e Estados Unidos já assinaram o tratado). Ela contém normas processuais e penais a respeito dessa espécie de crime. O texto abaixo foi retirado do site do Conselho: (http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=12&DF=2/11/05&CL=ENG) e está disponível, também em francês.

CONVENTION ON CYBERCRIME
Budapest, 23.XI.2001

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 parties 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 cybercrime, *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 by 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 cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action 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 their detection, investigation and prosecution at both the domestic and international levels 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 and 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 right to the protection of personal data, as conferred, for example, 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 evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. 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, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. 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, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions 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 cybercrime;

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 and 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 interconnected 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:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii 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 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 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.ii of this article.

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 person 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 person.

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 person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term “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, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and 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 revising 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 (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 through 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, and 9.1.a and c. of this Convention.

3 Each Party 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 legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, 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 In addition to the cases already provided for in paragraph 1 of this article, 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 through 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 provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 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 procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of 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, each 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 ninety 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 and 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.

2 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, the term “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 and by which can be established:

a the type of 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 a 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, the 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;

d 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 the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to 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 transmitted in its territory, through the 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 the execution of any power provided for in this article and any information relating to it.

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 the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to 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 on specified communications in its territory through the 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 the execution of any power provided for in this article and any information relating to it.

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 through 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 Party 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 through 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 or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its 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 the 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 through 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 for 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 address of each authority responsible for making or receiving requests 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 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, 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 through 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 denominate 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 and 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 only 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 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, 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 responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission 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 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 the grounds for refusal established in 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. Reasons shall be given for any refusal or postponement of the request. 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 of any request made under this chapter as well as its subject, except to the extent necessary for its execution. 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 sub-paragraph a. of this article 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 exists, 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 supply 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 should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies 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 reservation of data stored by means of a computer system, 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 seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying 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 stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons 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 sixty 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 a 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 pursuant to 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 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 the 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 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 in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this 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 in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under 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 twenty-four hour, seven-day-a-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 the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision 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 which is 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.

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 State 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 Paris, 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 have otherwise 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 Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to 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 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes 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, encouraging them to take appropriate action to give them effect.

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, and Article 41, paragraph 1. 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 of the Council of Europe. 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 of the Council of Europe 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 CDPC and, following consultation with the non-member States 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 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 cybercrime 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 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 40 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 Budapest, this 23rd day of November 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.