COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 26.1.2001
COM(2000) 890 final

COMUNICAÇÃO DA COMISSÃO AO CONSELHO, AO PARLAMENTO EUROPEU, AO COMITÉ ECONÓMICO E SOCIAL E AO COMITÉ DAS REGIÕES

Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade

Resumo

A transição da Europa para a sociedade da informação é marcada por profundas alterações que afectam todos os aspectos da vida humana: o trabalho, a educação e os tempos livres, a administração pública, a indústria e o comércio. As novas tecnologias da informação e da comunicação têm um impacto profundo e fundamental nas nossas economias e nas nossas sociedades. O êxito da sociedade da informação é importante para o crescimento, a competitividade e a criação de emprego na Europa e tem repercussões consideráveis do ponto de vista económico, social e jurídico.

A Comissão lançou a iniciativa *e*Europa em Dezembro de 1999 com o objectivo de permitir que a Europa beneficie das vantagens das tecnologias digitais para fazer com que a sociedade da informação emergente constitua um factor de integração social. Em Junho de 2000, o Conselho Europeu da Feira adoptou um plano global de acção sobre a iniciativa *e*Europa e solicitou a sua implementação até ao final de 2002. Este plano de acção sublinha a importância de que se reveste a segurança das redes e a luta contra a cibercriminalidade.

As infra-estruturas da informação e da comunicação tornaram-se uma componente crucial das nossas economias. Infelizmente, estas infra-estruturas têm as suas próprias vulnerabilidades e proporcionam novas oportunidades a comportamentos criminosos. Estas actividades criminosas podem assumir formas muito variadas e podem atravessar muitas fronteiras. Apesar de, por inúmeras razões, não existirem estatísticas fiáveis, não há qualquer dúvida de que estas infracções constituem uma ameaça para os investimentos e os activos das empresas, bem como para a segurança e confiança na sociedade da informação. Sabe-se que alguns exemplos recentes de negação de serviço e de ataques de vírus causaram graves prejuízos financeiros.

Podem prever-se várias acções quer em termos de prevenção das actividades criminosas, reforçando a segurança das infra-estruturas da informação, quer dotando os serviços responsáveis pela aplicação da lei dos meios adequados para agir, respeitando no entanto plenamente os direitos fundamentais dos indivíduos.

A União Europeia adoptou já inúmeras medidas para lutar contra as mensagens com conteúdo ilegal e lesivo na Internet, para proteger os direitos de propriedade intelectual e os dados pessoais, para promover o comércio electrónico bem como a utilização das assinaturas electrónicas e para reforçar a segurança das transacções. Em Abril de 1998, a Comissão apresentou ao Conselho os resultados de um estudo sobre a cibercriminalidade (denominado "COMCRIME"). Em Outubro de 1999, o Conselho Europeu de Tampere concluiu que os esforços destinados a chegar a um acordo sobre definições e sanções comuns deveriam incidir também sobre a criminalidade que utiliza tecnologias de ponta. O Parlamento Europeu convidou igualmente à criação de definições da criminalidade informática aceitáveis para todos bem como a uma aproximação efectiva das legislações, em especial relativamente ao direito penal substantivo. O Conselho da União Europeia adoptou para além disso uma posição comum relativa às negociações respeitantes ao projecto de Convenção do Conselho da Europa em matéria de cibercrime e adoptou um certo número de medidas iniciais no âmbito da estratégia da União para lutar contra a criminalidade que utiliza tecnologias de ponta. Alguns Estados-Membros da UE desempenharam igualmente um papel primordial nas actividades do G8 nesta matéria.

A presente Comunicação analisa a necessidade de uma iniciativa tendo em vista a definição de uma política global e das diferentes formas que esta poderá assumir no contexto de objectivos mais vastos como a *Sociedade da Informação* e a criação de um espaço de *Liberdade, de Segurança e de Justiça*, de modo a melhorar a segurança das infra-estruturas da informação e de lutar contra a criminalidade informática, e em conformidade com o compromisso da União Europeia de respeitar os direitos fundamentais dos indivíduos.

A Comissão considera que, a curto prazo, se verifica uma clara necessidade de adopção de um instrumento comunitário destinado a garantir que os Estados-Membros dispõem de sanções eficazes para combater a pornografia infantil na Internet. A Comissão introduzirá até ao final do ano uma proposta de decisão-quadro que incluirá disposições destinadas à aproximação das legislações e das sanções, no contexto mais amplo de um pacote de medidas que abrangerá questões associadas à exploração sexual de crianças e ao tráfico de seres humanos,.

A mais longo prazo, a Comissão apresentará propostas legislativas para uma aproximação mais aprofundada do direito penal material em matéria de criminalidade que utiliza tecnologias avançadas. Em conformidade com as conclusões do Conselho Europeu de Tampere de Outubro de 1999, a Comissão tomará também em consideração as opções para o reconhecimento mútuo das decisões anteriores à fase de julgamento no quadro de investigações sobre a cibercriminalidade.

Paralelamente, a Comissão tenciona promover, a nível nacional, a criação de unidades policiais especializadas na luta contra a criminalidade informática, onde estas ainda não existam, apoiar acções de formação técnica apropriadas para os serviços responsáveis pela aplicação d a lei e incentivar acções europeias em matéria de segurança da informação.

A nível técnico e em conformidade com o enquadramento jurídico, a Comissão promoverá os esforços de I&D destinados a compreender e a reduzir as vulnerabilidades e incentivará a divulgação do saber-fazer.

A Comissão tenciona também criar um fórum sobre a criminalidade informática a nível da União Europeia que agrupará os serviços responsáveis pela aplicação da lei, os fornecedores de serviços de Internet, os operadores de telecomunicações, as organizações de defesa das liberdades públicas, os representantes dos consumidores, as autoridades responsáveis pela protecção dos dados e outras partes interessadas com o objectivo de reforçar a compreensão mútua e a cooperação a nível da União Europeia. O fórum procurará aumentar a consciencialização pública para os riscos da criminalidade na Internet, promover as melhores práticas em matéria de segurança, definir instrumentos e procedimentos eficazes a fim de lutar contra a criminalidade informática, bem como incentivar a adopção de medidas tendo em vista mecanismos de alerta rápido e de gestão das crises.

CONVITE À APRESENTAÇÃO DE OBSERVAÇÕES À PRESENTE COMUNICAÇÃO

A Comissão Europeia gostaria de receber observações de todas as partes interessadas relativamente às questões abordadas na presente comunicação, que podem ser enviadas até 23.03.2001 por correio electrónico para o seguinte endereço:

Infso-jai-cybercrime-comments@cec.eu.int

As observações serão em princípio publicadas na *web*, a menos que o seu autor solicite expressamente que não pretende a sua publicação. As observações anónimas não serão publicadas. A Comissão reserva-se o direito de não publicar as observações que receber (por exemplo, devido ao facto de as observações incluírem linguagem ofensiva). As observações estarão disponíveis através de um *link* no seguinte endereço:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Encontrar-se-ão neste sítio da *web* sugestões quanto ao formato técnico e pormenores da política de publicações. É aconselhável consultar este sítio antes de enviar as observações.

AUDIÇÃO PÚBLICA

A Comissão Europeia organizará igualmente uma audição pública das partes interessadas relativamente às questões abordadas na Comunicação. Esta audição realizar-se-á em 07.03.2001. Os pedidos para a apresentação de uma declaração na audição podem ser enviados até 20.02.2001 por correio electrónico para o seguinte endereço:

Infso-jai-cybercrime-hearing@cec.eu.int

Ou pelo correio para o seguinte endereço:
Comissão Europeia
Gabinete BU 33-5/9
200 Wetstraat/Rue de la Loi
B- 1049 Bruxelas
Bélgica

A Comissão Europeia reserva-se o direito de proceder à selecção das partes a serem ouvidas. Qualquer selecção será baseada no número de pedidos e pretende ter uma ampla cobertura de interesses.

ÍNDICE

1. OPORTUNIDADES E AMEAÇAS NA SOCIEDADE DA INFORMAÇÃO

A crescente disponibilidade e utilização das tecnologias da sociedade da informação (TSI) bem como a mundialização da economia são características do período em que vivemos. Os progressos técnicos futuros e a maior utilização das redes abertas, tais como a Internet, nos próximos anos proporcionarão novas possibilidades mas colocarão também novos desafios.

O Conselho Europeu de Lisboa, de Março de 2000, sublinhou a importância da passagem para uma economia competitiva, dinâmica e baseada no conhecimento e convidou o Conselho e a Comissão a elaborarem um plano de acção *e*Europa a fim de tirar o melhor partido possível desta oportunidade[1]. Este Plano de Acção, elaborado pela Comissão e pelo Conselho, adoptado pelo Conselho Europeu da Feira de Junho de 2000, inclui acções destinadas a reforçar a segurança das redes e prevê o desenvolvimento de uma abordagem coordenada e coerente da criminalidade informática até ao final de 2002[2].

As infra-estruturas da informação tornaram-se uma parte primordial da estrutura das nossas economias. Os utilizadores deverão poder dispor de serviços de informação e ter confiança que as suas comunicações e os seus dados serão preservados contra qualquer acesso ou alteração não autorizada. Disto depende a generalização do comércio electrónico e a plena realização da sociedade da informação.

As novas tecnologias digitais e sem fios estão já omnipresentes. Oferecem-nos mobilidade, continuando a estar ligados a uma variedade de serviços acessíveis através de redes de redes. Dão-nos também a possibilidade de participar, ensinar e aprender, jogar e trabalhar em conjunto e tomar parte na vida política. Contudo, à medida que as sociedades se tornarem mais dependentes desta técnica, será necessário utilizar meios práticos e jurídicos eficientes para ajudar a gerir os riscos associados a esta evolução.

As Tecnologias da Sociedade da Informação (TSI) podem ser utilizadas, e são-no efectivamente, para realizar e facilitar diversas actividades criminosas. Nas mãos de pessoas que agem de má fé, por maldade ou por grave negligência, estas tecnologias podem tornar-se instrumentos de actividades que põem em perigo ou lesam a vida, os bens ou a dignidade das pessoas ou prejudicam mesmo o interesse público.

A abordagem clássica em matéria de segurança exigia uma compartimentação rigorosa do ponto de vista organizacional, geográfico e estrutural das informações em função da sua sensibilidade e categoria. Esta abordagem deixou de ser realmente viável no mundo digital, uma vez que o processamento da informação está fragmentado, os serviços seguem utilizadores móveis e a interoperabilidade dos sistemas constitui uma condição prévia. Soluções inovadoras baseadas nas técnicas emergentes estão a substituir as abordagens tradicionais em matéria de segurança. Incluem a utilização de codificação e de assinaturas digitais, novos instrumentos do controlo de acesso e de autenticação e uma vasta gama de filtros informáticos[3]. A fim de conferir segurança e fiabilidade às infra-estruturas da

---

1 Conclusões da Presidência do Conselho Europeu de Lisboa de 23 e 24 de Março de 2000, disponíveis no sítio http://ue.eu.int/pt/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_pt.htm.

3 Os fluxos de informação são filtrados e controlados a todos os níveis, desde a protecção (*firewall*) que examina os pacotes de dados, passando pelo filtro que procura eventuais programas informáticos hostis, o filtro do correio electrónico que elimina discretamente os correios electrónicos não solicitados (*spam*), até ao filtro do navegador que impede qualquer acesso a conteúdo prejudiciais.

informação, é necessário não apenas dispor de um leque completo de técnicas, mas igualmente operacionalizá-las correctamente e utilizá-las de forma eficaz. Algumas destas técnicas existem já, mas os utilizadores ignoram muitas vezes a sua existência, a forma de as utilizar ou as razões pelas quais se podem tornar necessárias.

1.1. Respostas nacionais e internacionais

A criminalidade informática ou cibercrime afecta todo o ciberespaço e não pára nas fronteiras tradicionais dos Estados. Estas infracções podem, em princípio, ser cometidas a partir de qualquer ponto e contra qualquer utilizador de computador, independentemente do local onde se encontra. Reconhece-se de uma forma geral que se impõe uma acção eficaz, tanto a nível nacional como internacional, a fim de lutar contra a criminalidade informática.[4]

A nível nacional, faltam ainda muitas vezes respostas adequadas e orientadas para uma dimensão internacional a fim de dar resposta aos novos desafios que constituem a segurança das redes e a criminalidade informática. Na maior parte dos países, as reacções a este tipo de delinquência são centradas no direito nacional (especialmente no direito penal), e negligenciam as outras medidas de prevenção.

Apesar dos esforços das organizações internacionais e supranacionais, as legislações nacionais revelam diferenças significativas a nível mundial, em especial no que diz respeito às disposições de direito penal relativas à pirataria informática, à protecção de segredos comerciais e aos conteúdos ilícitos. Existem também importantes disparidades quanto aos poderes coercivos das entidades de investigação (especialmente no que diz respeito aos dados codificados e às investigações nas redes internacionais), à extensão das competências em matéria penal, bem como relativamente à responsabilidade dos fornecedores de serviços intermédios, por um lado, e dos fornecedores de conteúdo, por outro. A Directiva 2000/31/CE[5] relativa ao comércio electrónico altera esta situação no que diz respeito à responsabilidade dos fornecedores de serviços intermédios em relação a certas actividades intermédias. A Directiva proíbe igualmente os Estados-Membros de imporem a esses prestadores de serviços intermédios como obrigação geral da supervisão das informações que transmitem ou que armazenam.

A nível internacional e supranacional, a necessidade de combater eficazmente a criminalidade informática foi amplamente reconhecida e diversas organizações coordenam ou tentam harmonizar as actividades nesta matéria. Os ministros da Justiça e dos Assuntos Internos do G8 adoptaram um conjunto de princípios e um plano de acção em 10 pontos em Dezembro de 1997, que foi aprovado pela Cimeira do G8 de Birmingham em Junho de 1998 e que se encontra actualmente na fase de aplicação[6]. O Conselho da Europa começou em Fevereiro

---

4 Ver, por exemplo, o Plano de Acção *e*-Europa em http://europa.eu.int/comm/information_society/eeurope/actionplan/index_pt.htm, E declarações do Comissário Europeu António Vitorino em http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, E do Primeiro Ministro francês Lionel Jospin em http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da Sociedade de Informação, em especial do comércio electrónico, no mercado interno ("Directiva sobre o comércio electrónico").

6 O Conselho JAI da União Europeia de 19 de Março de 1998 aprovou os 10 princípios para combater a criminalidade associada à alta tecnologia e convidou os Estados-Membros da União Europeia não membros do G8 a tomarem disposições para aderirem a esta rede.

de 1997 a elaborar uma convenção internacional em matéria de cibercrime e deverá concluir os seus trabalhos em 2001[7]. O combate ao cibercrime encontra-se igualmente na ordem de trabalhos das discussões bilaterais que a Comissão Europeia realiza com alguns Governos (para além da UE). Foi criada uma Task Force conjunta CE/EUA em matéria de protecção das infra-estruturas críticas (Joint EC/US Task Force on Critical Infrastructure Protection).[8]

As Nações Unidas e a OCDE desenvolveram igualmente acções neste domínio que estão a ser discutidas em fóruns internacionais como o Diálogo Comercial Global e o Diálogo Comercial Transatlântico [9].

A nível da União Europeia, até recentemente, as medidas legislativas ocorreram no âmbito dos direitos de autor, da protecção do direito fundamental à privacidade e da protecção dos dados pessoais, dos serviços de acesso condicional, do comércio electrónico, das assinaturas electrónicas e em especial da liberalização do comércio nos produtos codificados, que estão indirectamente associados à criminalidade informática.

Foram igualmente tomadas nos últimos 3-4 anos algumas medidas não legislativas importantes. Trata-se nomeadamente do plano de acção contra as mensagens com um conteúdo ilegal e lesivo difundidas na Internet, que co-financia acções de sensibilização, experiências de filtragem e de classificação do conteúdo, bem como linhas directas ("*hot-lines*"), e iniciativas relativas à protecção dos menores e da dignidade humana na sociedade da informação, à pornografia infantil e à intercepção de comunicações pelos serviços autorizados[10]. A União Europeia apoia desde há muito projectos de I&D que se destinam a promover a segurança e a confiança nas infra-estruturas da informação e nas transacções electrónicas e aumentou recentemente as respectivas dotações orçamentais no programa TSI. Os projectos de investigação bem como os projectos operacionais destinados a

---

Disponível na Rede Judiciária Europeia no sítio http://ue.eu.int/ejn/index.htm

7 O projecto de convenção encontra-se acessível na rede em duas línguas, em francês: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm e em inglês: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

8 Sob os auspícios do Grupo Consultivo conjunto do Acordo de cooperação científica e tecnológica CE/EUA.

9 As Nações Unidas elaboraram um manual pormenorizado intitulado "Manual on the prevention and control of computer-related crime," que foi recentemente actualizado. Em 1983, a OCDE realizou um estudo sobre as possibilidades de uma aplicação e de uma harmonização internacionais das legislações penais a fim de resolver o problema da criminalidade informática ou dos abusos informáticos. Em 1986, publicou um relatório intitulado "Computer-Related Crime: Analysis of Legal Policy", passando em revista as legislações existentes e as propostas de reforma em alguns Estados-Membros e recomendando uma lista mínima dos abusos que os países deveriam proibir e sancionar no seu direito penal. Finalmente, em 1992, a OCDE elaborou um conjunto de orientações que regulamentam a segurança dos sistemas de informação, destinadas a servir de base para a criação, por parte dos Estados-Membros e do sector privado de um quadro para a segurança dos sistemas de informação.

10 Recomendação 98/560/CE do Conselho de 24 de Setembro de 1998 relativa ao desenvolvimento da competitividade da indústria europeia de serviços audiovisuais e de informação através da promoção de quadros nacionais conducentes a um nível comparável e eficaz de protecção dos menores e da dignidade humana; Livro Verde sobre a protecção dos menores e da dignidade da pessoa humana nos serviços audiovisuais e de informação; COM(96) 483, Outubro de 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm;
Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões – Conteúdo ilegal e lesivo na Internet (COM(96) 487 final);
Resolução relativa à comunicação da Comissão respeitante ao conteúdo ilegal e lesivo na Internet (COM(96) 487 - C4-0592/96);
Resolução do Conselho de 17 de Janeiro de 1995 relativa à intercepção legal de telecomunicações (JO C 329 de 4.11.1996, pp. 1-6).

promover a formação especializada de funcionários dos serviços responsáveis pela aplicação da lei bem como a cooperação entre estes serviços e as empresas têm sido igualmente apoiados no quadro dos programas do terceiro pilar tais como STOP, FALCONE, OISIN e GROTIUS[11].

O plano de acção de luta contra o crime organizado, adoptado pelo Conselho JAI em Maio de 1997 e aprovado pelo Conselho Europeu de Amsterdão, incluía um pedido para que a Comissão elaborasse até ao final de 1998 um estudo sobre a criminalidade informática. Este estudo, denominado "Estudo COMCRIME", foi apresentado pela Comissão ao Grupo Multidisciplinar do Conselho sobre a criminalidade organizada em Abril de 1998[12]. A presente comunicação constitui, em parte, um seguimento a esse pedido do Conselho JAI.

Antes de redigir a presente comunicação, a Comissão considerou apropriado realizar consultas informais com os representantes dos serviços dos Estados-Membros responsáveis pela aplicação da lei e das autoridades responsáveis pela supervisão dos dados pessoais[13], bem como com representantes das empresas europeias (na maior parte fornecedores de serviços Internet e empresas de telecomunicações)[14].

Com base na análise e nas recomendações apresentadas no estudo, nos resultados do processo de consulta, nas novas possibilidades proporcionadas pelo Tratado de Amsterdão e no trabalho realizado na UE, no G8 e no Conselho da Europa, a presente comunicação analisará as várias acções complementares a realizar pela UE para lutar contra a criminalidade informática. A nível da União Europeia, as soluções escolhidas não devem prejudicar a realização do mercado interno ou provocar a sua fragmentação nem conduzir a medidas que diminuam a protecção de direitos fundamentais[15].

2. SEGURANÇA DAS INFRA-ESTRUTURAS DA INFORMAÇÃO

Na Sociedade da Informação, as redes mundiais controladas pelos utilizadores estão gradualmente a substituir a antiga geração das redes de comunicação nacionais. Uma das razões que explica o êxito da Internet é que esta deu aos utilizadores acesso às técnicas mais modernas. A lei de Moore[16] prevê que a capacidade de computação duplicará de 18 em

---

11 http://europa.eu.int/comm/justice_home/jai/prog_pt.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME." O estudo foi realizado pelo Professor U. Sieber da Universidade de Würzburg através de um contrato celebrado com a Comissão Europeia. O relatório final está disponível no endereço: http://europa.eu.int/ISPO/legal/en/crime/crime.html.

13 A nível da UE, os serviços responsáveis pela supervisão da protecção dos dados constituem o grupo de trabalho relativo à protecção dos dados previsto no artigo 29º, que o órgão consultivo independente da UE relativo à protecção das pessoas no que diz respeito ao tratamento de dados pessoais, ver artigos 29º e 30º da Directiva 95/46/CE.

14 Realizaram-se em 10 de Dezembro de 1999 e 1 de Março de 2000 duas reuniões com os serviços responsáveis pela aplicação da lei. Realizou-se em 13 de Março de 2000 uma reunião com os representantes do sector da Internet e uma com um pequeno número de peritos de protecção de dados pessoais em 31 de Março de 2000, bem como uma reunião final com todos os representantes e peritos supramencionados em 17 de Abril de 2000. As actas das reuniões podem ser obtidas contactando: Comissão Europeia, Unidade INFSO/A5, ou para: Comissão Europeia, Unidade JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Bruxelas, Bélgica.

15 Carta dos Direitos Fundamentais da União Europeia (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), Artigo 6º do Tratado da União Europeia e jurisprudência do Tribunal de Justiça das Comunidades Europeias.

16 Esta observação foi formulada em 1965 por Gordon Moore, co-fundador da Intel, sobre o ritmo de progressão do número de transístores num circuito integrado. Actualmente este número duplica quase

18 meses. Ora, as técnicas de comunicação registam progressos ainda mais rápidos[17]. Uma das consequências desta evolução é que o volume dos dados transportados via Internet tem vindo a ser multiplicado por 2 em períodos inferiores a um ano.

As redes telefónicas tradicionais eram construídas e exploradas por organismos nacionais. Os utilizadores tinham uma escolha de serviços limitada e não exerciam qualquer controlo sobre este ambiente. As primeiras redes de transmissão de dados que foram criadas baseavam-se nesta mesma filosofia, ou seja, a do ambiente centralizado. Os sistemas de segurança desenvolvidos nesse ambiente reflectiam esta centralização.

A Internet e as outras redes novas são muito diferentes, de modo que os problemas de segurança devem ter soluções adaptadas a estes novos ambientes. Nessas redes, a informação e o controlo situam-se principalmente na periferia, onde se encontra o utilizador e os serviços. O núcleo da rede é simples e eficaz e tem essencialmente por missão transmitir dados. A verificação e o controlo do conteúdo são limitados dado que só intervêm no destino final onde os *bits* se transformam no som de uma voz, numa radiografia ou na confirmação de uma operação bancária. A segurança é por conseguinte, em grande medida, da responsabilidade do utilizador, uma vez que apenas este podem apreciar o valor dos *bits* que são enviados ou recebidos e determinar o nível de protecção necessária.

O ambiente do utilizador constitui por conseguinte um elemento-chave da infra-estrutura da informação. As técnicas de segurança têm de ser aí aplicadas com autorização e participação do utilizador e de acordo com as suas necessidades. Esta aplicação é tanto mais importante se considerarmos a gama cada vez maior de actividades que se podem realizar a partir de um mesmo terminal. Pode-se com efeito, a partir de um mesmo equipamento, trabalhar, jogar, ver televisão e autorizar transferências bancárias.

Já existem várias tecnologias em matéria de segurança e estão a ser desenvolvidas outras novas. As vantagens de um desenvolvimento de programas informáticos livres ou abertos sob o ponto de vista da segurança estão a tornar-se mais evidentes. No que diz respeito a métodos formais ou a critérios de avaliação da segurança já se verificaram progressos notáveis. A utilização de tecnologias de codificação e de assinaturas electrónicas está a tornar-se indispensável, em especial face ao crescimento do acesso sem fios. É necessária uma variedade cada vez maior de mecanismos de autenticação para dar resposta às nossas diferentes necessidades nos ambientes em que evoluímos. Em certos casos, com efeito, podemos ter necessidade, ou vontade, de manter o anonimato, enquanto noutros, podemos necessitar de ter de provar uma certa característica, embora não revelando a nossa identidade, tal como ser adulto, ou empregado ou cliente de uma determinada empresa. Ainda noutras situações, pode revelar-se necessário comprovar a nossa identidade. Também os filtros informáticos se estão a tornar cada vez mais sofisticados, permitindo-nos proteger-nos ou proteger as pessoas que estão a nosso cargo, de dados que não pretendemos, tais como conteúdos indesejáveis, correio electrónico não solicitado, programas informáticos hostis e outras formas de ataque. A aplicação e a gestão desses requisitos de segurança na Internet bem como nas novas redes implicam também despesas consideráveis para as empresas e os utilizadores. Por conseguinte, é importante incentivar a inovação e a utilização comercial de tecnologias e serviços de segurança informática.

---

de 18 em 18 meses, o que tem uma influência directa sobre o preço e os desempenhos das pastilhas informáticas. Inúmeros peritos consideram que esta lei se verificará ainda durante pelo menos nos próximos 10 anos.

[17] As tecnologias mais recentes permitem que um único cabo de fibras ópticas transporte simultaneamente o equivalente a 100 milhões de comunicações telefónicas.

Naturalmente, o facto de a infra-estrutura de ligações de comunicação e servidores de nome ser partilhada coloca também problemas a nível da segurança. A transmissão de dados depende das ligações físicas através das quais os dados são encaminhados de um computador para outro. Estas ligações têm de ser criadas e protegidas de modo que a transmissão continue a ser possível apesar de acidentes, ataques e de um volume cada vez maior de tráfego. As comunicações dependem também de serviços críticos tais como os fornecidos por servidores de nomes, e em especial do pequeno número de servidores de nomes de raiz que fornecem os endereços necessários. Em relação a cada uma destas componentes será igualmente necessário, , uma protecção adequada, que variará em função da parte do espaço de nome de domínio e da clientela a que este serviço é fornecido.

Impulsionadas pelo objectivo de dar uma maior flexibilidade e resposta às necessidades das pessoas, as tecnologias das infra-estruturas da informação tornaram-se cada vez mais complexas, mas dedicando frequentemente poucos esforços a nível da concepção de mecanismos de segurança. Além disso, esta complexidade envolve cada vez mais programas informáticos sofisticados e interligados, que por vezes incluem pontos fracos e lacunas a nível da segurança, que podem facilmente ser aproveitadas para ataques. À medida que o ciberespaço se torna cada vez mais complexo e as suas componentes mais sofisticadas, poderão surgir vulnerabilidades novas e imprevistas.

Existem já vários mecanismos tecnológicos, e estão a ser desenvolvidos outros, para melhorar a segurança no ciberespaço. Esta resposta tecnológica inclui medidas para:

- Garantir a segurança de elementos críticos das infra-estruturas através da utilização de infra-estruturas essenciais públicas (PKI), do desenvolvimento de protocolos de segurança, etc.

- Garantir a segurança de ambientes privados e públicos através do desenvolvimento de programas informáticos de qualidade, protecções (*firewalls*), programas antivírus, sistemas electrónicos de gestão de direitos, codificação, etc.

- Garantir a autenticação de utilizadores autorizados, a utilização de cartões inteligentes, a identificação biométrica, as assinaturas electrónicas, as tecnologias de acesso pela função, etc.

Tal exige um maior esforço no desenvolvimento de tecnologias de segurança, que envolva a cooperação entre as partes interessadas de modo a alcançar a necessária interoperabilidade entre soluções, através de acordos em matéria de normas internacionais.

É igualmente importante que qualquer futuro enquadramento conceptual de segurança informática seja parte integrante da arquitectura global, dando resposta a ameaças e vulnerabilidades desde o início do processo de concepção. Tal situação contrasta com as abordagens tradicionais, que tentam necessariamente encontrar soluções pontuais para colmatar as lacunas aproveitadas por organizações criminosas cada vez mais sofisticadas.

O programa comunitário relativo às tecnologias da sociedade de informação (TSI)[18], e em particular as acções consagradas à segurança da informação, das redes e às tecnologias que têm por objectivo suscitar a confiança[19], constitui um quadro de referência para o

---

[18] O programa TSI é gerido pela Comissão Europeia. Faz parte do 5º Programa-quadro, que cobre o período de 1998 a 2002. Para mais informações, consultar o sítio http://www.cordis.lu/ist.

[19] Na acção-chave 2 – Novos métodos de trabalho e comércio electrónico.

desenvolvimento das capacidades e das técnicas necessárias para compreender e dar resposta aos desafios que a criminalidade informática começa a colocar. Estas técnicas incluem nomeadamente instrumentos técnicos de protecção contra as violações dos direitos fundamentais de protecção da privacidade e dos dados pessoais e outros direitos das pessoas e de luta contra a criminalidade informática. Além disso, no contexto do programa TSI, foi lançada uma iniciativa relativa à confiança no funcionamento do sistema. Esta iniciativa contribuirá para suscitar a confiança em infra-estruturas muito interconectadas e em sistemas estreitamente ligados em rede, sensibilizando para o problema da confiança no funcionamento e incentivando as técnicas que a tornam possível. A cooperação internacional faz parte integrante desta iniciativa. O programa TSI desenvolveu relações de trabalho com a DARPA e a NSF e criou em ligação com o Departamento de Estado dos Estados Unidos uma Task Force conjunta Comunidade Europeia/Estados Unidos relativa à protecção das infra-estruturas críticas (Joint EC/US Task Force on Critical Infrastructure Protection)[20].

Finalmente, a execução das obrigações em matéria de segurança decorrentes em especial das Directivas comunitárias relativas à protecção de dados[21] contribui para reforçar a segurança das redes e o tratamento dos dados.

3. CRIMINALIDADE INFORMÁTICA

Os sistemas modernos de informação e comunicação oferecem a possibilidade de exercer actividades ilegais a partir de qualquer ponto do planeta e a qualquer momento. Não existem estatísticas fiáveis sobre a verdadeira extensão do fenómeno da criminalidade informática. O número de intrusões detectadas e assinaladas até hoje não dá verdadeiramente uma ideia exacta da gravidade do problema. A tomada de consciência e a experiência dos administradores de sistemas e dos utilizadores são ainda limitadas, pelo que grande número de intrusões não é detectado. Para além disso, muitas empresas não estão dispostas a assinalar os casos de abuso informático, para evitar uma má publicidade e não se exporem ao risco de novos ataques. Os serviços de polícia, na sua maior parte, não possuem ainda estatísticas relativas às utilizações de computadores e sistemas de comunicação implicados neste tipo e noutras formas de criminalidade. Contudo, é de prever um aumento do número de actividades ilegais à medida que a utilização dos computadores e das redes se intensifique. Verifica-se uma clara necessidade de reunir provas fiáveis no que se refere à importância da cibercriminalidade.

Na presente comunicação, a criminalidade informática é entendida num sentido lato, como qualquer infracção que, de uma forma ou de outra, implica a utilização de técnicas informáticas. Diferentes concepções se opõem contudo em relação ao que é abrangido por "criminalidade informática". As noções de "criminalidade informática", "delinquência informática", "criminalidade que utiliza tecnologias avançadas" e "cibercriminalidade" são frequentemente utilizadas de forma indiscriminada. Pode estabelecer-se uma distinção entre a criminalidade especificamente associada à informática e as infracções clássicas cometidas com a ajuda de técnicas informáticas. Pode verificar-se um exemplo concreto deste aspecto na área aduaneira, em que a Internet constitui um instrumento para cometer crimes típicos contra a legislação aduaneira, tais como, contrabando, contrafacção, etc. Na medida em que a criminalidade informática impõe uma actualização das definições das infracções nos códigos

---

[20] Sob a égide do grupo consultivo conjunto criado por força do acordo de cooperação científica e tecnológica entre a Comunidade Europeia e o Governo dos Estados Unidos da América.

[21] Ver artigo 4º da Directiva 97/66/CE (incluindo igualmente uma obrigação de informação sobre os riscos remanescentes em termos de segurança) e o artigo 17º da Directiva 95/46/CE.

penais nacionais, as infracções tradicionais cometidas com apoio informático tornam necessário um reforço e uma melhoria da cooperação internacional bem como a adopção de medidas processuais.

Todas estas infracções têm no entanto em comum o facto de explorarem as redes de informação e de comunicação existentes, que não conhecem fronteiras, bem como a circulação de dados que são intangíveis e extremamente voláteis. Estas características exigem um reexame das medidas existentes a fim de enfrentar as actividades ilícitas que se exercem nestas redes e nestes sistemas ou graças a eles.

Inúmeros países adoptaram uma legislação sobre a criminalidade informática. Nos Estados-Membros da União Europeia, foram já adoptados alguns instrumentos jurídicos. Ainda que, para além da Decisão do Conselho relativa à pornografia infantil na Internet, não se disponha até agora de qualquer instrumento jurídico comunitário que trate directamente a criminalidade informática, existem alguns instrumentos que são indirectamente aplicáveis nesta matéria.

Os principais problemas abordados na legislação em relação ao domínio específico da criminalidade informática, tanto a nível da União Europeia como dos Estados-Membros, são os seguintes:

Violações da vida privada: vários países adoptaram uma legislação penal relativa à recolha, armazenamento, modificação, divulgação e disseminação ilícitas de dados pessoais. A nível da União Europeia, existem duas Directivas que aproximam as legislações nacionais em matéria de protecção da vida privada no âmbito do tratamento de dados pessoais[22]. O artigo 24º da Directiva 95/46/CE obriga claramente os Estados-Membros a adoptarem todas as medidas adequadas para garantir a plena aplicação das disposições da directiva, incluindo a aplicação de sanções no caso de infracções às disposições constantes da legislação nacional. Além disso os direitos fundamentais à vida privada e a protecção dos dados estão inseridos na Carta dos Direitos Fundamentais da União Europeia.

Infracções ligadas aos conteúdos: a divulgação, em especial na Internet, de imagens pornográficas, nomeadamente sobre pornografia infantil, declarações racistas e informações que incitam à violência suscitam a questão de saber até que ponto o direito penal podia permitir combater tais actos. A Comissão considerou que o que é ilícito "fora de linha" deve sê-lo igualmente em linha. A responsabilidade penal dos autores ou dos fornecedores de conteúdo[23] pode ser posta em causa. O Conselho adoptou uma decisão sobre o combate à pornografia infantil na Internet[24]. A responsabilidade dos prestadores de serviços intermédios, cuja redes ou servidores são utilizados para transmitir ou armazenar informações de terceiros, é tratada pela directiva relativa ao comércio electrónico.

---

22 Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e a Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. O artigo 24º da Directiva 95/46/CE obriga os Estados-Membros a determinarem as sanções a aplicar em caso de violação das disposições relativas à protecção de dados.

23 O fornecedor de conteúdo não deve ser confundido com o prestador ou fornecedor de serviços.

24 Decisão do Conselho de 29 de Maio de 2000 sobre o combate à pornografia infantil na Internet (JO L 138 de 9.6.2000, p.1).

Infracções económicas, acesso não autorizado e sabotagem: inúmeros países adoptaram legislação sobre a criminalidade informática que define novas infracções ligadas ao acesso não autorizado aos sistemas informáticos (por exemplo, pirataria informática, sabotagem informática e difusão de vírus, espionagem informática, falsificação informática ou fraude informática[25]) e novas formas de realização de infracções (por exemplo, procedendo a manipulações informáticas em vez de enganar uma pessoa). O objecto do crime é frequentemente intangível, isto é, dinheiro em depósitos bancários ou programas informáticos. Actualmente, não existem quaisquer instrumentos a nível comunitário que tratem destes tipos de actividade ilegal. No que se refere à prevenção, a revisão da regulamentação relativa aos produtos duais recentemente adoptada contribuiu de forma significativa para generalizar a disponibilidade de produtos codificados.

Violações da propriedade intelectual: Foram adoptadas duas directivas relativas à protecção jurídica dos programas de computador e das bases de dados[26], que dizem directamente respeito à sociedade da informação e prevêem sanções nestes domínios. Foi adoptada pelo Conselho uma posição comum respeitante a uma proposta de Directiva relativa aos direitos de autor e aos direitos conexos na Sociedade da Informação. Prevê-se que seja adoptada no início de 2001[27]. A violação dos direitos de autor e dos direitos conexos bem como a neutralização dos meios técnicos criados para proteger estes direitos devem ser sancionadas. No que diz respeito à contrafacção e à pirataria, a Comissão apresentará, até ao final do ano 2000, uma comunicação que fará o balanço do processo de consulta lançado com a publicação do Livro Verde de 1998 e que anunciará um plano de acção nesta matéria. À medida que a Internet assume cada vez maior importância a nível comercial, começam a surgir novos tipos de litígios relativos ao registo abusivo de nomes de domínios relativos à ciberocupação (*cybersquatting)*, ao açambarcamento (*warehousing*) e à apropriação abusiva (*reverse hijacking)* e, naturalmente, há também quem reclame a adopção de regras e de procedimentos que contribuam para a resolução destes problemas[28].

É necessário abordar também a questão do respeito das obrigações de carácter fiscal. No caso das transacções comerciais, em que o beneficiário do fornecimento em linha de um serviço electrónico se encontra situado na UE, tal dará origem na maior parte dos casos a obrigações

---

25 Os meios de comunicação deram muita atenção aos recentes ataques de "negação de serviço distribuído" de que foram vítimas grandes sítios na Internet e à divulgação do vírus denominado LoveBug. É contudo necessário ressituar o problema. Os ataques de negação de serviço, quer sejam deliberados ou acidentais, tal como os vírus transmitidos por correio electrónico surgiram há muitos anos. O vírus Morris e o vírus da árvore de Natal IBM são alguns exemplos mais antigos. Existem produtos e procedimentos para combater estes vírus. Existe também um bom espírito de cooperação na comunidade Internet para limitar os prejuízos que tais ataques podem provocar no momento em que se produzem. Existe uma cooperação semelhante para limitar os abusos associados à divulgação de mensagens não solicitadas.

26 Directiva 91/250/CEE do Conselho, de 14 de Maio de 1991, relativa à protecção jurídica dos programas de computador (JO L 122 de 17.5.1991, pp. 42 – 46).
Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de Março de 1996, relativa à protecção jurídica das bases de dados (JO L 77 de 27.3.1996, pp. 20 – 28).

27 Posição comum adoptada pelo Conselho tendo em vista a adopção de uma directiva do Parlamento Europeu e do Conselho relativa à harmonização de certos aspectos dos direitos de autor e dos direitos conexos na Sociedade da Informação (CS/2000/9512).

28 Comunicação da Comissão ao Conselho e ao Parlamento Europeu: A Organização e a Gestão da Internet – Questões de Política Internacional Europeia 1998–2000, Abril de 2000, COM(2000) 202.

fiscais no território em que se considera que se realiza o consumo desse serviço.[29] O não cumprimento das obrigações fiscais sujeita um operador a sanções civis (e em alguns casos penais) que podem incluir o congelamento de contas bancárias ou a apreensão de outros activos. Apesar de a opção preferível ser sempre o cumprimento voluntário, tais obrigações devem em última análise ter força executória.

A cooperação entre as administrações fiscais constitui o elemento principal para atingir este objectivo. No entanto, conferir a alguns a possibilidade de protegerem as suas transacções legais, dará também os mesmos meios a infractores para protegerem as suas transacções ilegais. Os instrumentos que nos dão um comércio electrónico seguro podem igualmente ser utilizados para apoiar o tráfico de drogas. É necessário identificar as prioridades e proceder a escolhas.

A protecção das vítimas da cibercriminalidade inclui também as questões relativas à responsabilidade, às vias de recurso e a indemnizações que ocorrem quando se verifica um crime informático. A confiança depende não apenas da utilização de uma tecnologia adequada, mas também da existência de garantias jurídicas e económicas que a acompanhem. Estas questões devem ser analisadas para o conjunto dos crimes informáticos.

Existe manifestamente uma necessidade de adopção de instrumentos eficazes de direito material e processual aproximados, senão a nível mundial, pelo menos a nível europeu, de maneira a proteger as vítimas da criminalidade informática e perseguir os autores dessas infracções. Paralelamente, as comunicações pessoais, a vida privada e a protecção dos dados, o acesso à informação e a respectiva divulgação constituem direitos fundamentais das democracias modernas. Esta é a razão pela qual seria necessário dispor e utilizar medidas de prevenção eficazes de forma a tornar menos necessárias as medidas repressivas. Qualquer medida legislativa que venha a ser necessária para combater a cibercriminalidade deverá encontrar um justo equilíbrio entre estes interesses importantes.

4. QUESTÕES DE DIREITO MATERIAL

A aproximação das disposições de direito material na área da criminalidade que utiliza tecnologias avançadas garantirá um nível mínimo de protecção para as vítimas da cibercriminalidade (por exemplo, vítimas da pornografia infantil), ajudará a cumprir o requisito de que uma actividade deve constituir um delito nos dois países antes de poder ser prestada uma assistência jurídica mútua para apoiar uma investigação criminal (o requisito da criminalidade dupla), e proporcionará uma maior clareza para as empresas (por exemplo, sobre o que se entende por conteúdo ilícito).

Na realidade, a adopção de um instrumento legislativo comunitário que aproxime o direito penal material em matéria de criminalidade informática figura entre as prioridades da União Europeia desde o Conselho Europeu de Tampere de Outubro de 1999[30]. O Conselho inscreveu a criminalidade que utiliza as tecnologias avançadas numa lista limitada de sectores em que

---

29 A Comissão propôs uma série de alterações ao regime IVA da UE destinadas a clarificar o local de imposição (COM (2000) 349 - Proposta de directiva do Conselho que altera a Directiva 77/388/CEE no que se refere ao regime do imposto sobre o valor acrescentado aplicável a determinados serviços prestados por via electrónica) actualmente em análise no Conselho e no Parlamento. Nalgumas circunstâncias, contudo, a responsabilidade de pagar impostos pode incumbir ao fornecedor, mesmo quando este não tem uma presença física no território de tributação.

30 http://db.consilium.eu.int/pt/Info/eurocouncil/index.htm.

devem ser desenvolvidos esforços para se chegar a um acordo relativamente a definições, incriminações e sanções comuns. Este tipo de criminalidade figura também na Recomendação nº 7 da Estratégia da União Europeia relativa à prevenção e repressão da criminalidade organizada para o próximo milénio, adoptada pelo Conselho "Justiça e Assuntos Internos" em Março de 2000[31]. Insere-se igualmente no programa de trabalho da Comissão para 2000 e no painel de avaliação relativo à criação de um espaço de liberdade, de segurança e de justiça, apresentado pela Comissão e adoptado pelo Conselho "Justiça e Assuntos Internos" em 27 de Março de 2000[32].

A Comissão acompanhou os trabalhos da Convenção do Conselho da Europa em matéria de cibercrime. Este projecto de Convenção do Conselho da Europa em matéria de cibercrime inclui, na sua versão actual, quatro categorias de infracções penais: 1) infracções contra a confidencialidade, a integridade e a disponibilidade dos dados e sistemas informáticos; 2) infracções informáticas; 3) infracções relativas aos conteúdos e 4) infracções associadas às violações da propriedade intelectual e dos direitos conexos.

A aproximação a nível comunitário poderá ser mais abrangente do que a prevista na Convenção do Conselho da Europa, que representa uma aproximação internacional mínima. Poderá estar operacional mais rapidamente do que o tempo necessário para que a Convenção do Conselho da Europa entre em vigor[33]. Integrará a criminalidade informática no âmbito do direito comunitário e criará mecanismos comunitários de controlo da aplicação do direito.

A Comissão dá grande importância ao facto de dotar a União Europeia de meios de acção eficazes, em especial contra a pornografia infantil na Internet. Congratula-se com a decisão do Conselho relativa ao combate à pornografia infantil neste sector, mas partilha o parecer do Parlamento Europeu segundo o qual são ainda necessárias medidas complementares a fim de aproximar as legislações nacionais. Tenciona apresentar até ao final do ano uma proposta de decisão-quadro do Conselho que incluirá disposições destinadas a uma aproximação das legislações e sanções aplicáveis à pornografia infantil na Internet[34].

Em conformidade com as conclusões de Tampere, a Comissão apresentará uma proposta legislativa ao abrigo do Título VI do Tratado da UE com o objectivo de aproximar as definições de infracções que utilizam tecnologias avançadas. Tal basear-se-á nos progressos alcançados no Conselho da Europa, e dará especialmente resposta à necessidade de aproximar as legislações relativas aos ataques de pirataria e negação de serviço. A proposta incluirá definições-tipo para a União Europeia nesta área, e poderá ir ainda mais longe do que o projecto de Convenção do Conselho da Europa, garantindo que os casos graves de ataques de pirataria e de negação de serviço são minimamente sancionados em todos os Estados-Membros.

---

31 Prevenção e controlo da criminalidade organizada: Estratégia da União Europeia para o início do novo milénio (JO C 124 de 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_pt.htm.

33 A Convenção do Conselho da Europa só poderá entrar em vigor após a sua ratificação.

34 Esta iniciativa faz parte de um conjunto de propostas que abrange igualmente problemas mais vastos associados à exploração sexual das crianças e ao tráfico de seres humanos, tal como a Comissão tinha anunciado na sua Comunicação de Dezembro de 1998 relativa ao tráfico de seres humanos. O texto da proposta de uma decisão-quadro do Conselho encontra-se em anexo à Comunicação da Comissão ao Conselho e ao Parlamento Europeu relativa à luta contra o tráfego de seres humanos e a exploração sexual de crianças: duas propostas de decisões-quadro, que são publicadas paralelamente à Comunicação.

Além disso, a Comissão explorará as possibilidades de lutar contra o racismo e a xenofobia na Internet, tendo em vista a apresentação de uma proposta de decisão-quadro do Conselho ao abrigo do Título VI do Tratado da UE que abranja as actividades xenófobas fora de linha e em linha. Esta acção terá em conta os resultados da próxima avaliação da aplicação, por parte dos Estados-Membros, da acção comum de 15 de Julho de 1996 relativa à acção contra o racismo e a xenofobia[35]. A Acção comum constituiu um primeiro passo para a aproximação dos delitos relativos ao racismo e à xenofobia, mas é necessária uma aproximação mais aprofundada na União Europeia. A importância e o carácter sensível desta questão foram sublinhados pela decisão de um tribunal francês em 20 de Novembro de 2000, que exigiu que o Yahoo impedisse que os utilizadores franceses tivessem acesso a sítios de venda de objectos nazis[36].

Finalmente, a Comissão reflectirá sobre a forma de reforçar a eficácia dos esforços da luta contra o comércio de drogas ilícitas na Internet, cuja importância foi reconhecida na estratégia antidroga da União Europeia 2000-2004, aprovada pelo Conselho Europeu de Helsínquia[37].

5. QUESTÕES DE DIREITO PROCESSUAL

A própria natureza das infracções informáticas coloca, quer a nível nacional quer internacional, o problema dos procedimentos aplicáveis, na medida em que afectam soberanias, competências e legislações diferentes. Mais do que em relação a qualquer outra forma de criminalidade transnacional, a rapidez, a mobilidade e a flexibilidade da criminalidade informática desafiam as regras existentes em matéria de direito penal processual.

A aproximação dos poderes em matéria de direito processual reforçará a protecção das vítimas garantindo que as autoridades responsáveis pela aplicação da lei têm os poderes de que necessitam para investigar infracções no seu próprio território, e que conseguem responder rapida e eficazmente a pedidos de cooperação de outros Estados-Membros.

É igualmente importante assegurar que as medidas tomadas com base no direito penal, que geralmente são da competência dos Estados-Membros e abrangidas pelo Título VI do Tratado da União Europeia estejam em conformidade com os requisitos do direito comunitário. Em especial, o Tribunal de Justiça tem alegado constantemente que essas disposições legislativas não podem proceder a uma discriminação em relação a pessoas às quais a legislação comunitária dá o direito a um tratamento equitativo nem restringir as liberdades fundamentais garantidas pelo direito comunitário.[38]Quaisquer novos poderes para aplicação da legislação devem ser apreciados à luz do direito comunitário e do seu impacto sobre a vida privada.

---

35 JO L 185 de 24.7.1996, p. 5-7. Igualmente disponível no sítio da Rede Judiciária Europeia http://ue.eu.int/ejn/index.htm.

36 Tribunal de Grande Instância de Paris, decisão em processo de urgência proferida em 20 de Novembro de 2000, No. RG 00/05308

37 Plano de Acção comunitário antidroga (2000–2004). COM(1999)239 final. http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

38 Processo C-274/96 Bickel & Franz (1998) Col. I-7637 ponto 17, Processo C-186/87 Cowan (1989) Col. 195 ponto 19. Em especial, as medidas administrativas ou sanções devem ir mais além do que é estritamente necessário, os procedimentos de controlo não devem ser concebidos de forma a restringir a liberdade exigida pelo Tratado e não devem ser acompanhados de uma sanção, que seja tão desproporcionada em relação com a gravidade da infracção que se torne um obstáculo ao exercício dessa liberdade (Processo C-203/80 Casati (1981) Col. 2595 ponto 27).

5.1. Intercepção das comunicações

Na União Europeia, existe um princípio geral de confidencialidade das comunicações (e respectivos dados relativos ao tráfego). As intercepções são ilegais a menos que sejam autorizadas por lei quando necessárias em casos específicos para efeitos limitados. Tal decorre do artigo 8º da Convenção Europeia dos Direitos do Homem, a que se refere o artigo 6º do Tratado da União Europeia e mais especialmente das Directivas 95/46/CE e 97/66/CE.

Todos os Estados-Membros criaram um enquadramento jurídico que permite aos serviços responsáveis pela aplicação da lei obterem decisões judiciais (ou, no caso de dois Estados-Membros, uma garantia autorizada a título pessoal por um Ministro) para a intercepção das comunicações na rede pública de telecomunicações[39]. Esta legislação, que deve estar em conformidade com a legislação comunitária na medida em que esta seja aplicável, prevê garantias rigorosas para proteger os direitos fundamentais das pessoas no que diz respeito à sua vida privada, por exemplo, limitando o recurso à intercepção das comunicações para efeitos de instrução de casos de infracções graves e exigindo que, em cada uma destas investigações, a intercepção seja necessária e proporcional e garantindo que os indivíduos sejam informados sobre a intercepção, desde que tal não impeça a investigação. Em inúmeros Estados-Membros, a legislação relativa à intercepção das comunicações prevê a obrigação de as empresas de telecomunicações (que asseguram o serviço público) darem possibilidades de proceder a estas escutas. Uma Resolução do Conselho de 1995 tinha por objectivo coordenar as especificações em matéria de intercepção[40].

Os operadores tradicionais de redes, em especial os que fornecem serviços de telefonia vocal, estabeleceram já no passado relações de trabalho com os serviços responsáveis pela aplicação da lei de modo a facilitar a intercepção legal das telecomunicações. A liberalização das telecomunicações e a explosão da utilização da Internet atraíram muitas empresas novas ao mercado, às quais foram impostas de novo obrigações em matéria de intercepção. Será necessário discutir, no âmbito do diálogo entre as entidades públicas e as empresas, questões relativas à regulamentação, à viabilidade técnica, à repartição dos custos e ao impacto comercial. Este diálogo deverá incluir todas as outras partes implicadas incluindo as autoridades de supervisão da protecção dos dados.

As novas tecnologias tornam indispensável uma cooperação entre os Estados-Membros, caso estes pretendam manter a possibilidade de interceptar legalmente as comunicações. A

---

39 Dois Estados-Membros não reconhecem as comunicações interceptadas como elementos de prova nos processos penais.

40 Resolução do Conselho de 17 de Janeiro de 1995 relativa à intercepção legal de telecomunicações (JO C 329 de 4.11.1996, pp. 1-6). O anexo inclui uma lista das especificações dos serviços autorizados em matéria de intercepção que os Estados-Membros eram convidados a ter em conta aquando da definição e da aplicação das políticas e das medidas nacionais aplicáveis na matéria. Em 1998, a Presidência austríaca propôs uma Resolução do Conselho da União Europeia destinada a alargar o âmbito de aplicação da Resolução de 1995 às novas tecnologias, nomeadamente à Internet e às comunicações por satélite. Esta questão foi objecto de debate no âmbito de duas comissões do Parlamento Europeu, ou seja, a Comissão das Liberdades e dos Direitos dos Cidadãos, da Justiça e dos Assuntos Internos e a Comissão dos Assuntos Jurídicos e do Mercado Interno, tendo as duas chegado a conclusões diferentes. A primeira Comissão considerou com efeito esta resolução como uma clarificação e uma actualização da antiga, tendo-a considerado aceitável. A segunda, por outro lado, formulou acérrimas críticas, tanto na perspectiva das potenciais violações dos direitos do homem como na perspectiva do custo económico para os operadores, o que a levou a rejeitar a proposta do Conselho e a convidar a Comissão a elaborar uma nova proposta logo que o Tratado de Amsterdão entre em vigor. Desde então, o projecto de resolução do Conselho não foi objecto nos últimos meses de um exame aprofundado pelo Conselho nem pelos seus grupos de trabalho.

Comissão considera que, se os Estados-Membros impuserem às empresas de telecomunicações e aos fornecedores de serviços Internet novas obrigações técnicas em matéria de intercepção, estas normas deverão ser objecto de uma coordenação internacional de maneira a evitar falsear o mercado interno e de reduzir ao mínimo os custos que implicam para as empresas, bem como respeitar os requisitos em termos de privacidade e de protecção dos dados. Estas normas devem ser transparentes e tornadas públicas, sendo caso disso, mas não devem introduzir deficiências nas infra-estruturas de comunicação.

No âmbito da Convenção da União Europeia relativa ao auxílio judiciário mútuo em matéria penal[41], foi acordado facilitar a cooperação em matéria de intercepção legal[42]. A Convenção inclui disposições relativas à intercepção das comunicações telefónicas por satélite[43], e à intercepção das comunicações estabelecidas por uma pessoa que se encontre no território de um outro Estado-Membro[44]. A Comissão considera que as regras em matéria de intercepção da Convenção de auxílio judiciário mútuo é, actualmente, o máximo que se pode obter. O texto da Convenção é neutro a nível tecnológico. Seria por conseguinte necessário testá-lo para avaliar a forma como esta funciona na prática antes de prever a introdução de quaisquer melhoramentos. A Comissão examinará os resultados da sua aplicação com os Estados-Membros, as empresas, os utilizadores e as autoridades de supervisão da protecção dos dados de forma a garantir a eficácia, a transparência e o justo equilíbrio das iniciativas tomadas nesta matéria.

Qualquer exploração das possibilidades de intercepção feita de forma abusiva e sem discernimento, em especial à escala internacional, colocaria problemas a nível dos direitos do homem e destruiria a confiança do cidadão na Sociedade da Informação. A Comissão alarmou-se com certos relatórios de que teve conhecimento relativamente a pretensos abusos dos meios de intercepção[45].

---

41 JO C 197 de 12.7.2000, p. 1. A Convenção foi adoptada em 29 de Maio de 2000. As disposições em matéria de intercepção da Convenção só são aplicáveis aos Estados-Membros da União Europeia e não aos países terceiros.

42 A Convenção prevê um mínimo de garantias no que se refere à protecção da vida privada e dos dados pessoais.

43 O objecto inicial das negociações consistia em dar possibilidades de intercepção de comunicações estabelecidas por pessoas que utilizam um telefone por satélite e que se encontram no território do Estado-Membro de intercepção. A nível técnico, o ponto nevrálgico para interceptar este tipo de comunicações é a nível da estação terrestre. Era por conseguinte necessário solicitar a assistência técnica do Estado-Membro no território do qual se encontra situada essa estação terrestre. A convenção prevê duas possibilidades para solucionar este problema: um procedimento acelerado de auxílio judiciário mútuo, que passa por pedidos de assistência pontuais dirigidos ao Estado-Membro que possui essa estação terrestre e uma solução técnica que assenta no acesso à distância à estação terrestre realizada pelo Estado-Membro de intercepção e que não exige qualquer pedido.

44 A Convenção constitui igualmente uma quadro jurídico para os pedidos de intercepção de comunicações estabelecidas por uma pessoa que se encontre no território de um outro Estado-Membro (o Estado-Membro a que foi feito o pedido). Neste caso, o Estado-Membro que intercepta e o Estado-Membro a que foi feito o pedido devem ambos obter uma decisão ou um mandato de intercepção ao abrigo do seu direito nacional respectivo. Finalmente, a Convenção estabelece as regras aplicáveis às situações em que o Estado-Membro de intercepção pode ter a possibilidade de interceptar as comunicações de uma pessoa que se encontre no território de um outro Estado-Membro sem ter que solicitar a assistência técnica desse Estado-Membro.

45 Um relatório longo e muito circunstanciado do Sr. Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) relativo a uma rede de intercepção de informações denominada ECHELON foi objecto de uma audição pública perante o Parlamento Europeu. O relatório especifica que o sistema ECHELON foi concebido para efeitos das necessidades de segurança nacional mas serviu igualmente para acções de espionagem industrial. O Parlamento Europeu criou uma

5.2. Retenção dos dados relativos ao tráfego

Para poder instruir e accionar as infracções que impliquem a utilização das redes de comunicação, nomeadamente a Internet, os serviços responsáveis pela aplicação da lei servem-se frequentemente dos dados relativos ao tráfego que os fornecedores de serviços armazenam para efeitos de facturação. Uma vez que o preço das comunicações está cada vez menos associado à distância e ao destino, e que os fornecedores de serviços evoluem para uma facturação fixa, a necessidade de armazenar os dados relativos ao tráfico para efeitos de facturação tende a desaparecer. Os serviços responsáveis pela aplicação da lei temem ver assim diminuir os elementos materiais potencialmente úteis para as investigações penais e reclamam por conseguinte que os fornecedores de serviços conservem esses dados durante um período mínimo a fim de lhes permitir utilizá-los para efeitos de repressão[46].

Em conformidade com as directivas comunitárias relativas à protecção dos dados pessoais e mais precisamente ao princípio geral de limitação das transferências para uma finalidade específica enunciado na Directiva 95/46/CE e nas disposições específicas incluídas na Directiva 97/66/CE, os dados relativos ao tráfego devem ser apagados ou tornados anónimos a partir do fornecimento da comunicação, salvo se forem necessários para efeitos de facturação. No caso de um acesso fixo ou gratuito aos serviços de telecomunicações, os fornecedores de serviços não estão autorizados, em princípio, a conservar os dados relativos ao tráfego.

Por força destas mesmas directivas, os Estados-Membros podem adoptar medidas legislativas destinadas a limitar o âmbito desta obrigação de eliminação dos dados relativos ao tráfego, nomeadamente quando essa limitação constituir uma medida necessária à prevenção, investigação, detecção e repressão de infracções penais e à utilização não autorizada do sistema de telecomunicações[47].

No entanto, qualquer medida legislativa tomada a nível nacional que possa prever a retenção dos dados relativos ao tráfego para fins de aplicação da lei deve satisfazer determinadas condições. Com efeito as medidas propostas devem ser apropriadas, necessárias e proporcionais, tal como exigido pelo direito comunitário e pelo direito internacional, incluindo as Directivas 97/66/CE e 95/46/CE, a Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais de 4 de Novembro de 1950 e na Convenção do Conselho da Europa, de 28 de Janeiro de 1981 relativa à protecção das pessoas face ao tratamento automatizado dos dados pessoais. O respeito destas condições e destes princípios é ainda mais importante no que se refere às medidas que implicam a retenção sistemática dos dados relativamente a uma grande parte da população.

Certos Estados-Membros tomam iniciativas de ordem legislativa ou regulamentar para obrigar ou autorizar os fornecedores de serviços a armazenarem determinadas categorias de dados relativos ao tráfego após o fornecimento do serviço.

---

comissão temporária encarregada de estudar a questão e apresentará um relatório dentro de um ano em sessão plenária.

46 Tal inclui as investigações penais nos processos que não têm qualquer relação com a informática ou com as redes de comunicação mas em que estes dados podem ajudar a identificar o autor da infracção.

47 Artigo 14º da Directiva 97/66/CE e artigo 13º da Directiva 95/46/CE.

Esses dados não são necessários para efeitos de facturação, , mas são considerados úteis para investigações penais. O alcance e a forma destas iniciativas variam muito consoante os Estados, mas partem todas do princípio de que os serviços responsáveis pela aplicação da lei devem necessitar de mais dados do que os disponíveis se os fornecedores de serviços tratassem apenas os dados estritamente necessários para as suas prestações. A Comissão examina actualmente estas medidas à luz do direito comunitário em vigor.

O Parlamento Europeu está atento aos problemas de protecção da vida privada e declarou-se em geral favorável a um elevado nível de protecção dos dados pessoais. Todavia, aquando dos debates sobre o combate contra a pornografia infantil na Internet, manifestou-se adepto de uma obrigação geral de retenção dos dados relativos ao tráfego durante um período de três meses[48].

Este parecer ilustra toda a importância do contexto em que se insere o exame de um assunto tão sensível quanto o da manutenção dos dados relativos ao tráfego e ao desafio a que devem fazer face as entidades responsáveis pela tomada de decisões nos seus esforços de procura de um justo equilíbrio.

A Comissão considera que qualquer solução para o problema complexo da manutenção dos dados relativos ao tráfego deve ser bem fundamentada, proporcional ao seu objectivo e conciliar de forma equitativa os interesses divergentes em causa. Só uma abordagem que agrupe a experiência e as capacidades dos poderes públicos, das empresas, das autoridades responsáveis pela supervisão da protecção dos dados e dos utilizadores conseguirá alcançar estes objectivos. Seria altamente desejável uma abordagem coerente em todos os Estados-Membros de modo a satisfazer os objectivos de eficácia e proporcionalidade e evitar uma situação em que os serviços responsáveis pela aplicação da legislação e a comunidade da Internet fossem confrontados com toda uma panóplia de enquadramentos técnicos e jurídicos.

Há que tomar em consideração interesses diferentes, mas igualmente importantes . Por um lado, as autoridades responsáveis pela supervisão da protecção dos dados consideraram que o meio mais eficaz para reduzir riscos inaceitáveis para a vida privada seria que os dados relativos ao tráfego não sejam em princípio apenas mantidos para efeitos de respeito da lei[49], reconhecendo simultaneamente a necessidade de uma aplicação eficaz da legislação. Os serviços responsáveis pela aplicação da lei, por seu lado, declararam que a manutenção de um serviço mínimo de dados sobre o tráfego durante um período mínimo seria necessário para facilitar as investigações penais.

As empresas têm interesse em cooperar no combate à criminalidade do tipo pirataria ou fraude informática, mas não se devem ver confrontadas com medidas que impliquem um custo exagerado. O impacto económico de quaisquer medidas deve ser cuidadosamente analisado e comparado com a sua eficácia no combate ao cibercrime para evitar que a Internet

---

48 Resolução legislativa sobre o parecer do Parlamento Europeu relativa ao projecto de acção comum – adoptado pelo Conselho com base no artigo K.3 do Tratado da União Europeia – sobre o combate à pornografia infantil na Internet, Alteração 17 (JO C 219 de 30.7.1999, p. 68 e nomeadamente p. 71).

49 "Deve ser proibida uma fiscalização exploratória ou geral em grande escala. […]o meio mais eficaz de reduzir riscos inadmissíveis em termos de privacidade, embora reconhecendo a necessidade de assegurar a aplicação eficaz da lei, é que os dados de tráfego não sejam mantidos em princípio apenas para esse efeito e que as legislações nacionais não devem obrigar os operadores de telecomunicações e os fornecedores de serviços de telecomunicações e de serviços Internet a manter esses dados por um período superior ao necessário para efeitos de facturação", Recomendação 3/99 de 7 de Setembro de 1999 do grupo de trabalho relativo à protecção dos dados previsto no artigo 29º, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

seja mais dispendiosa e menos abordável para os utilizadores. Seria necessário garantir uma segurança suficiente dos dados sobre o tráfego conservados desta forma.

De qualquer modo, as empresas terão um papel chave a desempenhar contribuindo para o processo de criação de uma Sociedade da Informação mais segura. Será necessário que os utilizadores tenham confiança na segurança da Sociedade da Informação e se sintam ao abrigo das infracções e das violações da sua vida privada.

A Comissão apoia e incentiva sem reservas a criação de um diálogo construtivo entre os serviços responsáveis pela aplicação da lei, as empresas, as autoridades responsáveis pela protecção dos dados e as organizações de consumidores, bem como com outras partes susceptíveis de estarem implicadas. No âmbito do fórum da União Europeia proposto pela presente Comunicação (ver ponto 6.4), a Comissão convidará todas as partes interessadas a procederem, prioritariamente, a um exame aprofundado da questão complexa da manutenção dos dados relativos ao tráfego, tendo em vista encontrar em comum soluções apropriadas, equilibradas e proporcionais, respeitando plenamente os direitos fundamentais à vida privada e à protecção dos dados[50]. Com base nos resultados deste exame, a Comissão poderá avaliar a necessidade de adoptar medidas legislativas ou de outro tipo a nível da União Europeia.

5.3. Acesso e utilização anónimos

Os especialistas das questões de repressão manifestaram receio de que o anonimato dê origem à ausência de responsabilidade e impeça perigosamente a prisão de certos autores de infracções. A utilização anónima do telefone móvel é possível em alguns países graças a cartões pré-pagos (mas não em todos). O acesso e utilização anónimos da Internet são propostos por determinados fornecedores de serviços ou de acesso, nomeadamente os reexpedidores anónimos e os cibercafés. O sistema de atribuição dinâmica dos endereços ip, em que os endereços não são afectados aos utilizadores a título permanente mas apenas durante uma determinada sessão, facilita igualmente uma certa forma de anonimato.

Nas suas discussões com a Comissão, alguns representantes das empresas manifestaram-se hostis a um anonimato total, em parte por razões associadas à sua própria segurança, ao combate contra a fraude e à integridade das redes. O London Internet Exchange publicou orientações relativamente às melhores práticas na matéria que se revelaram muito úteis no Reino Unido[51], e assinalou-as à Comissão no âmbito das discussões acima mencionadas. Todavia, outros representantes das empresas e peritos privados declararam que sem anonimato não é possível garantir os direitos fundamentais.

O grupo de trabalho relativo à protecção dos dados previsto no artigo 29º publicou uma recomendação sobre a questão do anonimato na Internet[52]. Considera que esta questão se encontra no âmago de um dilema ao qual os governos e as organizações internacionais devem fazer face. Por um lado, a possibilidade de permanecer anónimo é essencial para salvaguardar os direitos fundamentais à privacidade e à liberdade de expressão no ciberespaço. Por outro, a capacidade de participar e de comunicar em linha, sem revelar a respectiva

---

50 Tal como inserido na Convenção Europeia dos Direitos do Homem (artigo 8º, direito à vida privada), na Carta Europeia dos Direitos Fundamentais, no Tratado da União Europeia e nas Directivas comunitárias relativas à protecção dos dados.

51 http://www.linx.net/noncore/bcp/

52 Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais, Recomendação 3/97 – O anonimato na Internet, adoptado pelo grupo em 3 de Dezembro de 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

identidade, contraria o espírito das iniciativas desenvolvidas actualmente no intuito de apoiar outros aspectos fundamentais tais como o combate ao conteúdo ilegal e lesivo, à fraude financeira ou às violações dos direitos de autor. Este conflito aparente entre diferentes objectivos de interesse geral não é novo. No contexto dos meios de comunicação fora de linha mais tradicionais, tais como os correios e os serviços de expedição de encomendas, o telefone, os jornais ou a rádio e a televisão, foi assegurado um equilíbrio. Hoje em dia, o desafio a enfrentar pelos responsáveis políticos consiste em assegurar que esta abordagem equilibrada, que garante os direitos fundamentais permitindo simultaneamente restrições proporcionadas em circunstâncias restritas e específicas, seja mantida no novo quadro do ciberespaço. O alcance e os limites da capacidade de um indivíduo participar em linha de forma anónima serão determinantes para este equilíbrio.

Na declaração de encerramento da Conferência de Ministros sobre as redes globais de informação que se realizou em Bona de 6 a 8 de Julho de 1997, o princípio defendido foi que o utilizador deve poder escolher entre permanecer anónimo em linha quando tem a mesma escolha fora de linha. Existe por conseguinte um nítido consenso sobre o facto de as actividades exercidas nas redes deverem ser encaradas aplicando os princípios jurídicos de base aplicáveis noutros domínios. A Internet não é um gueto anárquico sem regras sociais. Contudo, a capacidade das administrações e dos poderes públicos de limitar os direitos dos particulares e de vigiar os comportamentos potencialmente ilícitos não deve ser maior nas redes públicas do que nas actividades fora de linha. A obrigação segundo a qual as restrições às liberdades e direitos fundamentais devem ser devidamente justificadas, necessárias e proporcionais em relação aos outros objectivos de ordem pública, deve igualmente ser aplicável no ciberespaço.

Na recomendação do grupo de trabalho relativo à protecção dos dados criado por força do artigo 29º é indicada de forma pormenorizada o modo de aplicar essa obrigação em casos específicos (por exemplo, no que diz respeito ao correio electrónico, aos fóruns de discussão, etc.)[53]. A Comissão associa-se às posições manifestadas pelo grupo.

5.4. Medidas concretas da cooperação a nível internacional

Recentemente, operações de repressão realizadas conjuntamente a nível mundial, tais como "Starburst" e "Cathedral" contra redes pedófilas, demonstraram que é útil que os serviços responsáveis pela aplicação da lei e o poder judicial coordenem a sua acção à escala internacional, tanto no que diz respeito à troca de informações na fase preliminar como impedindo os outros membros das redes sejam prevenidos no momento das detenções e das apreensões. A Internet demonstrou ser igualmente um utensílio valioso e eficaz para efeitos de investigações policiais e aduaneiras, quando é utilizada como um instrumento para cometer infracções tradicionais, tais como a contrafacção e o contrabando.

Por outro lado, estas operações evidenciaram as graves dificuldades jurídicas e operacionais com que se confrontam os serviços responsáveis pela aplicação da lei e as autoridades judiciárias na condução desta acção, tais como a preparação de uma comissão rogatória internacional, e a identificação das vítimas, bem como o papel das organizações intergovernamentais responsáveis pelas questões de polícia (Interpol e Europol, em especial).

---

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

No âmbito das medidas concretas de cooperação internacional, as redes internacionais de intercâmbio de informações estão a tornar-se cada vez mais importantes para as autoridades policiais e aduaneiras.

A nível do G8, foi criada e encontra-se já operacional uma rede de informações acessível 24 horas por dia e 7 dias na semana, que agrupa pontos de contacto competentes em matéria de repressão. A sua missão consiste essencialmente em recolher os pedidos urgentes de cooperação em processos em que intervêm provas electrónicas e de lhes dar resposta. Esta rede foi utilizada com êxito em alguns processos. O Conselho JAI de 19 de Março de 1998 aprovou os 10 princípios do combate à criminalidade organizada que utiliza tecnologias avançadas, adoptados pelo G8 e convidou os Estados-Membros da União Europeia não membros do G8 a aderirem a esta rede[54]. Estes pontos de contacto deverão praticar uma colaboração directa, que completará as estruturas de auxílio mútuo e os canais de comunicação existentes[55].

O projecto de Convenção do Conselho da Europa prevê igualmente a criação de uma rede deste tipo. A menção de uma rede de pontos de contacto que funciona 24 horas por dia e 7 dias na semana figura também na decisão do Conselho sobre o combate à pornografia infantil na Internet e na posição comum da União Europeia relativa ao projecto de Convenção do Conselho da Europa em matéria de cibercrime[56], bem como na decisão do Conselho que aprova o plano de acção do G8[57], mas a União Europeia não tomou até agora quaisquer medidas concretas relativamente a este assunto.

Dado que este domínio exige competências apropriadas e uma acção rápida, afigura-se urgente, segundo a Comissão, aplicar as intenções do Conselho. Para poder funcionar de forma eficaz, esta rede deve contudo dispor de um pessoal jurídico e tecnicamente competente o que exige medidas de formação correspondentes.

Verifica-se uma necessidade semelhante de intensificar a cooperação e o intercâmbio de informações entre autoridades aduaneiras. As formas de cooperação existentes devem ser reforçadas e desenvolvidos novos meios de gestão de operações conjuntas e de intercâmbio de informações. Tendo em devida conta os requisitos relativos à protecção dos dados, existe um consenso crescente entre as autoridades aduaneiras no sentido de se criarem redes de informação internacionais a fim de facilitar ainda mais o intercâmbio de informações. Sente-se igualmente uma necessidade de investir mais recursos nesta área, tanto no que diz respeito à melhoria dos sistemas informáticos como na formação de pessoal, para que as autoridades aduaneiras cumpram as suas tarefas de forma mais eficaz.

---

54 Para além dos membros do G8, cinco Estados-Membros da UE aderiram até agora à rede 24/7 do G8.

55 Aquando do Congresso mundial contra a exploração sexual das crianças para fins comerciais, que se realizou em Estocolmo em 28 de Agosto de 1996, foram apresentadas propostas tendo em vista integrar a INTERPOL nas redes supracitadas. A decisão do Conselho da União Europeia sobre o combate à pornografia infantil na Internet prevê igualmente a intervenção da Europol neste domínio.

56 Nº 1 do artigo 4º da posição comum: "Os Estados-Membros devem apoiar a definição de disposições que facilitem tanto quanto possível a cooperação internacional, incluindo disposições relativas ao auxílio judiciário mútuo. A Convenção deve facilitar a cooperação rápida no domínio de infracções informáticas ou por meios informatizados. Esta forma de cooperação poderá incluir a criação de pontos de contacto policiais que funcionem em permanência para complementar as estruturas de auxílio mútuo existentes."

57 Disponível no sítio da Rede Judiciária Europeia http://ue.eu.int/ejn/index.htm.

5.5. Poderes e competências em matéria de direito processual

A nível nacional e uma vez que estão preenchidas as condições legais necessárias, os serviços responsáveis pela aplicação da lei devem estar em condições de procurar e apreender dados armazenados em computadores bastante rapidamente a fim de impedir a destruição das provas de infracção penal. Os serviços responsáveis pela aplicação da lei consideram que devem dispor de poderes coercivos suficientes para poderem, no quadro das suas competências, proceder a buscas em sistemas informáticos e apreender dados, intimar pessoas a comunicar determinados dados informáticos, ordenar ou obter a rápida manutenção de dados exactos, em conformidade com as garantias e procedimentos jurídicos normais. Contudo, actualmente, as garantias e procedimentos não são objecto de qualquer aproximação.

Poderão colocar-se problemas se, aquando das suas buscas num computador, os serviços responsáveis pela aplicação da lei descobrirem que um certo número de computadores e de redes espalhados por todo o país se encontram implicados. Estas questões complicam-se ainda mais se, no momento de uma busca num computador ou de uma simples investigação, um serviço responsável pela aplicação da lei verificar que está em vias de consultar, ou que deve consultar, dados localizados num ou mais países. Como se encontram em jogo interesses fundamentais em termos de soberania, direitos do homem e aplicação da lei, seria conveniente conciliá-los da melhor forma.

Os instrumentos legais existentes em matéria de cooperação internacional em processos penais (auxílio judiciário mútuo) poderão revelar-se inadaptados ou insuficientes, uma vez que a sua aplicação leva normalmente vários dias, várias semanas ou mesmo vários meses. É necessário criar um mecanismo através do qual, no caso de processos penais transfronteiras, os países possam, com rapidez e eficácia, investigar infracções e recolher provas ou, pelo menos, não perder provas importantes, de uma forma compatível com os princípios de soberania nacional, dos direitos constitucionais e dos direitos do homem incluindo a protecção da vida privada e dos dados.

As novas propostas em análise no projecto de Convenção do Conselho da Europa em matéria de cibercriminalidade para solucionar estes problemas incluem decisões para a retenção de dados a fim de dar assistência a investigações específicas. Contudo, outras questões, tais como as buscas e as apreensões transfronteiras, apresentam dificuldades e questões em termos de formulação de políticas que ainda não foram resolvidas. Afigura-se claramente necessária um debate mais aprofundado entre todas as partes implicadas antes de poderem ser previstas quaisquer iniciativas concretas.

O subgrupo do G8 responsável pela criminalidade associada às tecnologias avançadas debateu a questão das buscas e apreensões transfronteiras e chegou a um consenso sobre princípios provisórios, na pendência da conclusão posterior de um acordo com um carácter mais permanente[58]. Colocam-se contudo questões importantes, nomeadamente sobre as condições em que é possível realizar buscas e apreensões no quadro de um processo acelerado, antes de informar do facto o Estado no qual estas se realizam. Devem ainda ser criadas as garantias apropriadas para respeitar os direitos fundamentais. Na sua posição comum relativa ao

[58] Comunicado da Conferência Ministerial dos países do G8 relativo ao combate ao crime organizado transnacional- Moscovo 19-20 Outubro de 1999 (ver http://www.usdoj.gov/criminal/cybercrime/action.htm e igualmente http://www.usdoj.gov/criminal/cybercrime/principles.htm)

projecto de Convenção do Conselho da Europa em matéria de cibercrime, os ministros do Conselho da União Europeia adoptaram uma posição aberta[59].

Nos casos de cibercriminalidade transfronteiras, é igualmente importante que existam regras claras sobre qual o país que é competente para actuar. Em especial, deve evitar-se situações em que nenhum país tenha competência. As principais regras propostas pelo projecto de Convenção do Conselho da Europa são que a competência seja estabelecida por um Estado quando a infracção é cometida no seu território ou por um dos seus cidadãos. Quando mais de um Estado reclama a competência, os Estados implicados devem proceder a consultas mútuas a fim de determinar a competência mais apropriada. Contudo, muito dependerá da eficácia das consultas bilaterais ou multilaterais. A Comissão continuará a analisar esta questão a fim de verificar se poderão ser necessárias outras medidas a nível comunitário.

A Comissão, que participou nas discussões do Conselho da Europa, tal como nas do G8, reconhece a complexidade destas questões e as dificuldades que acompanham as questões de direito processual. É contudo vital no âmbito da União Europeia que a luta contra o cibercrime seja realizada no âmbito de uma cooperação eficaz se se pretende tornar a sociedade da informação mais segura e criar um espaço de Liberdade, de Segurança e de Justiça.

A Comissão tenciona prosseguir as suas consultas com todas as partes implicadas durante os próximos meses, a fim de desenvolver estes trabalhos. Esta questão será igualmente examinada no contexto mais amplo das suas acções destinadas a aplicar as conclusões do Conselho Europeu de Tampere de Outubro de 1999. Em especial, o Conselho Europeu de Tampere solicitou ao Conselho e à Comissão que adoptassem, até Dezembro de 2000, um conjunto de medidas destinadas a aplicar o princípio do reconhecimento mútuo das decisões judiciais. A Comissão publicou já uma Comunicação relativa ao reconhecimento mútuo de decisões finais em matéria penal[60]. Como parte do seu contributo para aplicar a parte do programa de medidas relativas à execução de decisões anteriores à fase de julgamento, a Comissão estudará as possibilidades de reconhecimento mútuo das decisões que antecedem a fase de julgamento ligadas às investigações em matéria de cibercriminalidade tendo em vista a apresentação de uma proposta legislativa ao abrigo do Título VI do Tratado da União Europeia.

5.6. Validade probatória dos dados informáticos

Mesmo quando têm acesso a dados informáticos que parecem constituir provas de uma infracção penal, os serviços responsáveis pela aplicação da lei devem estar em condições de os recuperar e de os autenticar, de modo a poderem utilizá-los em investigações e acções penais. A sua tarefa é árdua, dada a volatilidade intrínseca dos dados electrónicos e a facilidade com que podem ser manipulados ou falsificados, tecnicamente protegidos ou destruídos. Este trabalho é confiado aos serviços de investigação da criminalidade informática, encarregados de desenvolverem e utilizarem protocolos e processos científicos

---

59 JO L 142, p. 2: "Sob reserva de princípios constitucionais e de salvaguardas específicas para respeitar devidamente a soberania, a segurança, a ordem pública ou outros interesses essenciais de outros Estados, poderá ser considerada a possibilidade de uma busca informática transfronteiras em casos excepcionais, nomeadamente em situações de emergência, por exemplo na medida em que tal seja necessário para evitar a destruição ou alteração de provas da infracção grave, ou para impedir que seja cometida uma infracção susceptível de provocar a morte ou danos corporais graves de pessoas".

60 COM (2000) 495, Bruxelas 26.7.2000.

para procurar provas informáticas e analisar e preservar a autenticidade dos dados que recuperaram.

A Organização Internacional das Provas Informáticas (International Organisation of Computer Evidence – IOCE) aceitou, a pedido dos peritos do G8, elaborar recomendações de normas, que incluam a definição de termos comuns, de métodos e de técnicas de identificação bem como a criação de um formato comum para os pedidos de natureza jurídica. Será necessário que a União Europeia seja associada a estes trabalhos, tanto a nível dos organismos dos Estados-Membros especializados nas investigações sobre a criminalidade informática como a nível da investigação e desenvolvimento financiada pelo 5º Programa-quadro (Programa TSI).

6. MEDIDAS NÃO LEGISLATIVAS

A aplicação de uma legislação apropriada a nível nacional e internacional afigura-se necessária, mas por si só não é suficiente para lutar de maneira eficaz contra a criminalidade informática e a utilização fraudulenta das redes. São igualmente necessárias algumas condições suplementares, não legislativas a fim de completar as medidas legislativas. A maior parte delas figura nas recomendações do estudo COMCRIME, bem como no plano de acção em dez pontos do G8, e tiveram a adesão de todas as partes que participaram no processo de consulta informal que precedeu a redacção da presente Comunicação. Esta condições incluem:

- a criação a nível nacional de unidades de polícia especializadas na luta contra a criminalidade informática, onde estas ainda não existam;

- a melhoria da cooperação entre os serviços responsáveis pela aplicação da lei, as empresas, as organizações de consumidores e as autoridades responsáveis pela protecção dos dados;

- medidas destinadas a incentivar as empresas e o meio associativo a tomarem iniciativas pertinentes, incluindo em matéria de produtos de segurança.

Neste contexto, a questão da codificação continuará provavelmente a ser importante. Trata-se de um instrumento indispensável para facilitar a criação e a adopção de novos serviços, incluindo o comércio electrónico, e pode desempenhar um papel não negligenciável na prevenção dos actos ilícitos na Internet. A política da Comissão em matéria de codificação foi apresentada na sua Comunicação relativa à segurança e à confiança nas comunicações electrónicas de 1997[61], em que a Comissão indicava que tentaria suprimir todas as restrições em matéria de livre circulação de todos os produtos codificados a nível da Comunidade Europeia. A Comunicação refere ainda que as restrições nacionais relativas à livre circulação de produtos codificados devem ser compatíveis com o direito comunitário e que a Comissão examinará se essas restrições nacionais são justificadas e proporcionais, nomeadamente no que diz respeito às disposições do Tratado em matéria de livre circulação, à jurisprudência do Tribunal de Justiça e aos requisitos constantes das Directivas relativas à protecção dos dados. Todavia, a Comissão reconhece que a codificação coloca também problemas novos e difíceis de resolver pelos serviços responsáveis pela aplicação da lei.

---

61 COM (97) 503.

A Comissão congratula-se por conseguinte com a adopção recente do novo regulamento sobre os bens duais, que contribuiu em grande medida para liberalizar o acesso aos produtos de codificação, admitindo simultaneamente que este movimento deve ser acompanhado por um reforço do diálogo entre os utilizadores, os profissionais e os serviços responsáveis pela aplicação da lei. A Comissão tenciona, por seu lado, incentivar este diálogo a nível comunitário propondo a criação do fórum da União Europeia sobre a criminalidade associada às tecnologias avançadas. A divulgação de produtos de segurança em toda a União Europeia, incluindo produtos de codificação robusta, se for caso disso, certificados com base em critérios de avaliação adaptados e aceites por todos, reforçará simultaneamente as possibilidades de prevenção de actos criminosos e a confiança dos utilizadores nas técnicas da sociedade da informação.

6.1. Unidades nacionais especializadas

Dada a complexidade jurídica e técnica de certas infracções informáticas, é indispensável constituir unidades especializadas a nível nacional. Estas unidades multidisciplinares (serviços responsáveis pela aplicação da lei e autoridades judiciárias), dotadas de pessoal com formação apropriada devem estar equipadas com instalações técnicas adequadas e funcionar enquanto pontos de contacto rápidos, tendo em vista:

- responder rapidamente aos pedidos de informações relativos a infracções presumidas. Será conveniente definir formatos comuns para trocar estas informações, mesmo que as discussões entre os peritos do G8 tenham demonstrado que as diferenças nacionais em matéria de culturas jurídicas ameaçavam dificultar esta tarefa;

- agir como interface para os serviços responsáveis pela aplicação da lei a nível nacional e internacional para as linhas directas[62] que recebem denúncias de utilizadores da Internet assinalando mensagens com conteúdo ilícito;

- melhorar e/ou desenvolver técnicas especializadas em matéria de investigação informática, a fim de detectar, instruir e reprimir os delitos informáticos;

- desempenhar o papel de centro de excelência sobre as questões da cibercriminalidade tendo em vista partilhar as melhores práticas e as experiências.

No âmbito da União Europeia, alguns Estados-Membros criaram já estas unidades especializadas na criminalidade informática. A Comissão considera que a criação destas unidades constitui uma prerrogativa dos Estados-Membros e incentiva vivamente estes últimos a tomarem medidas neste sentido. O custo que representam a compra de materiais e suportes lógicos mais recentes para estas unidades bem como a formação do seu pessoal é

---

62 Actualmente, só existem linhas directas num número limitado de países. De entre elas, citamos a Cybertipline nos Estados Unidos e a Internet Watch Foundation (IWF) no Reino Unido que criou, desde Dezembro de 1996, uma linha telefónica e um correio electrónico directo para que os utilizadores assinalem documentos encontrados na Internet e que considerem ilícitos. A IWF pronuncia-se sobre o carácter ilícito do documento, informa os fornecedores de serviços Internet e a polícia. Outros organismos de vigilância existem igualmente na Noruega (Redd Barna), nos Países Baixos (Meldpunt), na Alemanha (Newswatch, FSM e Jugendschutz), na Áustria (ISPAA) e na Irlanda (ISPAI). No quadro do programa comunitário Daphne, a Childnet International realiza actualmente um projecto directamente associado a esta questão ("International Hotline Providers in Europe Forum"). Do mesmo modo, os peritos da UNESCO reunidos em Paris em Janeiro de 1999 apoiaram e encorajaram a criação de linhas directas nacionais, a sua colocação em rede ou a criação de uma "vigilância electrónica internacional".

elevado e pressupõe que os poderes públicos, a nível competente estabeleçam prioridades e tomem as decisões políticas que se impõem[63]. As experiências das unidades existentes em alguns Estados-Membros poderão ser particularmente preciosas e a Comissão tomará medidas para incentivar o seu intercâmbio.

A Comissão considera igualmente que a Europol pode dar um valor acrescentado suplementar a nível comunitário, através de acções de coordenação, de análise e outras formas de assistência junto das unidades nacionais especializadas. A Comissão apoiará por conseguinte a extensão do mandato da Europol à cibercriminalidade.

6.2. Formação especializada

É necessário desenvolver esforços consideráveis no sector da formação permanente e especializada tanto dos profissionais dos serviços de polícia como dos serviços judiciários. As técnicas e os meios em matéria de delitos informáticos mudam mais rapidamente do que nos sectores mais clássicos da actividade criminosa.

Alguns Estados-Membros lançaram iniciativas para formar o pessoal dos serviços responsáveis pela aplicação da lei em tecnologias avançadas. Poderão dar conselhos e orientações aos Estados-Membros que ainda não tomaram medidas semelhantes.

Foram lançados com o apoio de programas geridos pela Comissão (em especial, STOP, FALCONE e GROTIUS) diversos projectos que vão nesse sentido, que assumem a forma de troca de experiências e de seminários consagrados aos desafios comuns com que se confrontam as categorias de profissionais em causa. A Comissão vai propor outras actividades neste domínio, nomeadamente no que diz respeito à formação em informática e à formação em linha.

A Europol tomou a iniciativa de acolher, em Novembro de 2000, uma sessão de formação de uma semana destinada ao pessoal dos serviços responsáveis pela aplicação da lei dos Estados-Membros, que incidiu nomeadamente sobre a pornografia infantil. O âmbito deste tipo de acção poderá ser alargado de forma a incluir a criminalidade informática em geral. A Interpol está igualmente presente neste sector há vários anos e poderá alargar as suas iniciativas na matéria a um maior número de participantes.

O G8 organizou acções que permitem a troca de experiências entre serviços responsáveis pela aplicação da lei e a elaboração de técnicas de investigação comuns a partir de casos concretos. Deverá ser lançada no segundo semestre de 2001 uma acção de formação suplementar. Os Estados-Membros da União Europeia que fazem parte do G8 poderão partilhar estas experiências com os outros Estados-Membros.

---

63 No que diz respeito à experiência americana neste domínio ver Michael A. Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", Duke Journal of Comparative and International Law, Vol. 9, Primavera de 1999, p. 464.

No domínio do combate à pornografia infantil na Internet, mais precisamente, da criação e gestão, a nível internacional, de uma biblioteca central digital das imagens de pornografia infantil (a que as unidades de polícia nacional especializadas teriam acesso por Internet, através da criação das condições e restrições necessárias em matéria de acesso e protecção da vida privada) facilitarão a procura das vítimas e dos culpados, contribuirão para classificar as infracções e para formar oficiais de polícia especializados[64].

6.3. Melhoria da informação e criação de regras comuns para a manutenção de registos

A harmonização das regras de manutenção de registos em matéria policial e judiciária bem como a criação de instrumentos adaptados à análise estatística da criminalidade informática ajudariam as autoridades responsáveis pela aplicação da lei e judiciárias a melhorar o armazenamento, a análise e a avaliação das informações oficiais recolhidas neste domínio, ainda em evolução.

Do mesmo modo, do ponto de vista do sector privado, tais estatísticas são necessárias para uma avaliação adequada dos riscos envolvidos, e uma análise custos-benefícios da sua gestão. Esta análise é importante não apenas por razões operacionais (tais como decidir sobre que medidas de segurança tomar) mas também para efeitos de seguros.

Está a ser actualizada e será colocada à disposição da Comissão uma base de dados que contém textos legislativos sobre a cibercriminalidade, e que faz parte do estudo COMCRIME. A Comissão prevê a melhoria do seu conteúdo (incluindo nela legislação, jurisprudência e publicações) bem como das suas condições de utilização**.**

6.4. Cooperação entre os vários intervenientes: o Fórum da União Europeia

A eficácia da cooperação entre os poderes públicos e as empresas no âmbito do enquadramento jurídico é considerado um elemento fundamental de qualquer política pública de luta contra a criminalidade informática[65]. Os representantes dos serviços responsáveis pela aplicação da lei concordaram que tinham, por vezes, dado provas de falta de clareza e de precisão ao indicar aos fornecedores de serviços as suas necessidades. Os representantes das empresas mostraram-se, no conjunto, favoráveis à melhoria da cooperação com os serviços responsáveis pela aplicação da lei, embora sublinhando a necessidade de encontrar um justo equilíbrio entre a protecção das liberdades e direitos fundamentais dos cidadãos e

---

64 Neste contexto, o projecto "Excalibur" lançado pela Direcção nacional sueca das informações em matéria de criminalidade com a ajuda da Comissão Europeia no âmbito do Programa STOP, deu muito bons resultados. Esta iniciativa foi lançada em colaboração com as forças de polícia alemãs, britânicas, neerlandesas e belgas, conjuntamente com a Europol e a Interpol. Foram também devidamente tidos em conta outros projectos desenvolvidos pela BKA alemã (o "Perkeo") e o Ministério Francês do Interior (projecto "Surfimage", co-financiado igualmente no âmbito do Programa STOP).

65 No Comunicado adoptado em Washington em 9 e 10 de Dezembro de 1997 sob os princípios e plano de acção em 10 Pontos da luta contra a criminalidade associada às tecnologias avançadas, os Ministros da Justiça e do Interior do G8 declararam: "são as empresas que concebem, aplicam e gerem estas redes mundiais e são as principais responsáveis pelo desenvolvimento das normas técnicas. Incumbe-lhes por conseguinte desempenhar o seu papel na elaboração e distribuição de sistemas de segurança concebidos para ajudar a identificar os casos de abuso informático, manter as provas electrónicas e facilitar a localização e identificação dos autores de infracções". A decisão do Conselho sobre o combate à pornografia infantil na Internet sublinha que é necessário que os Estados-Membros dêem início a um diálogo construtivo com as empresas e cooperem com elas partilhando as suas experiências.

nomeadamente o seu direito ao respeito da vida privada[66], a necessidade de lutar contra a criminalidade e as restrições económicas impostas aos fornecedores.

As empresas e os serviços responsáveis pela aplicação da lei podem, conjugando os seus esforços, sensibilizar o público para os riscos colocados pela criminalidade na Internet, incentivar as melhores práticas em matéria de segurança e elaborar instrumentos e procedimentos eficazes de luta contra a criminalidade. Foram já tomadas iniciativas nesse sentido por alguns Estados-Membros, das quais a mais antiga e mais ambiciosa é sem dúvida o fórum britânico da criminalidade na Internet (UK Internet Crime Fórum)[67].

A Comissão congratula-se com estas iniciativas e considera que devem ser incentivadas em todos os Estados-Membros. Projecta criar um fórum a nível da União Europeia que agrupe os serviços responsáveis pela aplicação da lei, fornecedores de serviços Internet, empresas de telecomunicações, organizações de defesa das liberdades públicas, representantes dos consumidores, autoridades responsáveis pela protecção de dados e outras partes interessadas, com o objectivo de intensificar e melhorar a cooperação a nível comunitário. Numa primeira fase, o Fórum incluirá funcionários nomeados pelos os Estados-Membros, peritos em tecnologia e especialistas em questões relativas ao respeito da vida privada designados pelo o grupo de trabalho relativo à protecção das pessoas no que diz respeito ao tratamento de dados pessoais criado por força do artigo 29º e representantes das empresas e dos consumidores escolhidos em estreita associação com as suas organizações representativas. Posteriormente, participarão igualmente neste fórum representantes de iniciativas nacionais tomadas na matéria.

O fórum da União Europeia será gerido de forma aberta e transparente, sendo publicados num sítio da *web* todos os documentos relevantes e todas as partes interessadas serão convidadas a apresentarem as suas observações.

O fórum da União Europeia será convidado em especial a reflectir sobre as seguintes acções:

- Criar, se for caso disso, pontos de contacto que funcionem 24 horas por dia entre os poderes públicos e as empresas;

- Desenvolver um formulário tipo adequado para os pedidos de informações dirigidos pelos serviços responsáveis pela aplicação da lei às empresas, e reforçar a utilização da Internet por esses serviços quando comunicam com os fornecedores de serviços;

- Incentivar a elaboração e/ou a aplicação dos códigos de conduta e de melhores práticas, bem como a sua utilização comum pelas empresas e os poderes públicos[68];

---

66 Tal como especificado nas directivas comunitárias relativas à protecção de dados, na Convenção do Conselho da Europa sobre os Direitos do Homem e na Convenção do Conselho da Europa nº 108 para a protecção das pessoas no que diz respeito ao tratamento automatizado dos dados pessoais, bem como na legislação nacional relevante.

67 Criado em 1997, o "Internet Crime Forum" agrupa oficiais de polícia, funcionários do Ministério britânico do Interior, responsáveis pela protecção dos dados e representantes do sector da Internet; este fórum realiza reuniões plenárias 3 ou 4 vezes por ano e dispõe de um certo número de grupos de trabalho permanentes.

68 No que diz respeito aos códigos de conduta na acepção do artigo 27º da Directiva 95/46/CE (poderiam abranger por exemplo questões ao abrigo da Directiva 97/66/CE, tais como as intercepções), estão envolvidos o grupo de trabalho relativo à protecção de dados previsto no artigo 29º e as autoridades nacionais responsáveis pela supervisão da protecção de dados.

- Promover a troca de informações entre as diversas partes, nomeadamente, entre as empresas e os serviços responsáveis pela aplicação da lei no que diz respeito às tendências em matéria de criminalidade que utiliza as tecnologias avançadas;

- Examinar as preocupações dos serviços responsáveis pela aplicação da lei sobre o desenvolvimento das novas tecnologias;

- Encorajar o desenvolvimento de mecanismos de alerta rápido e de gestão das crises a fim de prevenir, identificar e tratar as ameaças e as perturbações nas infra-estruturas de informação;

- Contribuir, se for caso disso, aos trabalhos em curso no âmbito do Conselho e outras instâncias internacionais, tais como o Conselho da Europa e o G8 em termos dos conhecimentos e da experiência acumulados,;

- Incentivar a cooperação entre as partes interessadas que inclua os princípios comuns aos serviços responsáveis pela aplicação da lei, às empresas e aos utilizadores (por exemplo, um Memorando de Acordo, Códigos de conduta em conformidade com o enquadramento jurídico).

6.5. Acções directamente realizadas pelas empresas

A luta contra a criminalidade informática é, em grande medida, do interesse de toda a colectividade. Se se pretende que os consumidores tenham confiança no comércio electrónico, as medidas para evitar a cibercriminalidade devem constituir um elemento de boa prática comercial amplamente aceite. Em inúmeros domínios, como serviços bancários, comunicações electrónicas, cartões de crédito e direitos de autor, as empresas e os seus clientes são vítimas potenciais da criminalidade informática. As empresas protegem naturalmente o seu próprio nome e as marcas comerciais, desempenhando por conseguinte um papel importante na prevenção da fraude. Certos organismos que representam o sector dos programas informáticos e dos fonogramas (British Phonographic Industry – BPI, por exemplo) dispõem de equipas encarregadas de inquirir sobre a pirataria (incluindo na Internet). Nalguns Estados-Membros os fornecedores de serviços Internet criaram linhas directas que permitem aos utilizadores denunciar as mensagens com conteúdo ilegal e lesivo.

A Comissão dá o seu apoio a algumas destas iniciativas incentivando a sua participação no Programa-quadro comunitário de Investigação e Desenvolvimento, na acção Internet[69] e nos programas abrangidos pelo Título VI, tais como STOP e DAPHNE.

O fórum da União Europeia permitirá o intercâmbio das melhores práticas nestes domínios.

6.6. Projectos de I&D financiados pela União Europeia

O programa de I&D sobre as tecnologias da Sociedade da Informação (TSI) que faz parte do 5º Programa-quadro 1998-2002, coloca o acento sobre o desenvolvimento e a utilização de tecnologias destinadas a suscitar a confiança. Do mesmo modo, estas últimas incluem simultaneamente a segurança das informações e das redes, bem como os meios técnicos e os métodos de protecção contra as violações do direito fundamental à vida privada e à protecção de dados, dos outros direitos individuais e da luta contra a cibercriminalidade.

---

[69] Para mais informações no que diz respeito ao Plano de Acção destinado a promover uma utilização mais segura da Internet consultar o endereço seguinte: http://158.169.50.95:10080/iap/.

O Programa TSI, em especial os trabalhos relativos à *Segurança das informações e das redes e outras tecnologias destinadas a suscitar a confiança* que constam da Acção-chave 2 – *Novos Métodos de Trabalho e Comércio Electrónico*, apresentam um quadro que permite desenvolver recursos e técnicas com o objectivo de compreender e dar resposta aos novos desafios tecnológicos associados à prevenção e à repressão da criminalidade informática e garantir que as exigências em matéria de segurança e privacidade possam ser satisfeitas a nível da União Europeia, das comunidades virtuais e do indivíduo.

Para além disso, de modo a abordar correctamente estes problemas de confiança, incluindo a prevenção e a instrução dos casos de criminalidade informática, foi igualmente lançada no âmbito do Programa TSI uma iniciativa sobre segurança de funcionamento. Esta iniciativa destina-se a reforçar e a garantir a confiança em infra-estruturas informáticas muito estreitamente interligadas e em sistemas incorporados e unidos em rede, sensibilizando simultaneamente para os problemas de confiança no funcionamento dos sistemas e encorajando as tecnologias que a tornam possível. A cooperação internacional faz parte integrante desta iniciativa. O Programa TSI desenvolveu relações de trabalho com a DARPA e a NSF e criou, em colaboração com o Departamento de Estado dos EUA uma Task Force conjunta sobre a protecção das infra-estruturas críticas, sob a égide do grupo consultivo conjunto criado no âmbito do acordo de cooperação científica e tecnológica Comunidade Europeia/Estados Unidos[70].

O Centro Comum de Investigação da Comissão (CCI), que apoia a iniciativa sobre a confiança no funcionamento no âmbito do programa TSI, esforçar-se-á principalmente por desenvolvermedidas, indicadores e estatísticas adaptadas e harmonizadas, em ligação com outras partes interessadas, incluindo a Europol. Esta acção terá por objecto classificar e compreender correctamente as actividades ilegais, a sua repartição geográfica, o seu ritmo de progressão e a eficácia das acções empreendidas para as combater. O CCI recorrerá, se for caso disso, a outros grupos de investigação e integrará os seus trabalhos e os seus resultados. Manterá um sítio Internet sobre esta questão e comunicará ao fórum da União Europeia a evolução alcançada nesta matéria.

7. CONCLUSÕES E PROPOSTAS

De maneira a prevenir a criminalidade informática e a lutar eficazmente contra este fenómeno, é necessário a existência prévia de algumas condições:

- disponibilidade de tecnologias em matéria de prevenção. Tal exige um quadro regulamentar adaptado que deixe campo livre à inovação e à investigação e as encoraje. O recurso ao financiamento público pode justificar-se para apoiar o desenvolvimento e a utilização de tecnologias de segurança apropriadas;

- sensibilização para os riscos potenciais associados à segurança e aos meios de os combater;

- disposições legislativas adequadas em matéria de direito material e processual, no que diz respeito às actividades criminosas tanto nacionais como transnacionais. A nível do direito penal material, as legislações nacionais devem ser suficientemente pormenorizadas e eficazes para incriminar as infracções informáticas graves e prever sanções dissuasoras,

[70] Encontram-se disponíveis mais informações relativas ao Programa TSI no seguinte endereço http://www.cordis.lu/ist.

contribuir para resolver os problemas de dupla infracção[71] e facilitar a cooperação internacional. Quando se justificar plenamente que os serviços responsáveis pela aplicação da lei procedam rapidamente a buscas, apreensões ou façam cópias com toda a segurança de dados informáticos no seu território nacional, a fim de poderem investigar uma infracção informática, o direito processual deverá permiti-lo, em conformidade com os princípios e as derrogações constantes do direito comunitário e da Convenção Europeia dos Direitos do Homem. A Comissão considera que o acordo relativo à intercepção das comunicações concluído no âmbito da Convenção relativa ao auxílio judiciário mútuo em matéria penal representa o máximo que é possível obter actualmente. A Comissão continuará a controlar a sua aplicação, com a ajuda dos Estados-Membros, das empresas e dos utilizadores, de modo a garantir que as iniciativas correspondentes são eficazes, transparentes e equilibradas;

- disponibilização de pessoal dos serviços responsáveis pela aplicação da lei, em número suficiente, com boa formação e correctamente equipado. Deverá ser ainda mais incentivada uma colaboração estreita com os fornecedores de serviços Internet e as empresas de telecomunicações em matéria de formação;

- reforço da cooperação entre todos os intervenientes interessados: utilizadores e consumidores, empresas, serviços responsáveis pela aplicação da lei e autoridades responsáveis pela protecção de dados. Esta condição afigura-se essencial para realizar uma investigação sobre a criminalidade informática e proteger a segurança pública. As empresas devem dispor de regras e obrigações claramente definidas. Os poderes públicos devem reconhecer que as necessidades dos serviços responsáveis pela aplicação da lei podem sobrecarregar as empresas e, por conseguinte, tomar medidas razoáveis para diminuir essa carga tanto quanto possível. Paralelamente, as empresas devem integrar nas suas práticas comerciais considerações de segurança pública. A cooperação e o apoio activo de utilizadores e de consumidores individuais serão neste aspecto cada vez mais necessárias;

- acções permanentes das empresas e do meio associativo. As linhas directas, que já se encontram em funcionamento para denunciar as mensagens com conteúdo ilegal ou lesivo, poderão ser alargadas a outras categorias de infracções. Medidas recomendadas pelo próprios profissionais bem como um protocolo de acordo pluridisciplinar poderão associar o maior número possível de partes interessadas e desempenhar um papel múltiplo na prevenção da cibercriminalidade e na luta contra este fenómeno, bem como numa melhor sensibilização e numa maior confiança por parte do público;

- é conveniente tirar o máximo partido dos resultados e das potencialidades da investigação e do desenvolvimento. A estratégia consistirá essencialmente em fazer coincidir a evolução das técnicas de segurança acessíveis e eficazes e outros meios para favorecer a confiança com as acções empreendidas a nível comunitário.

---

[71] Quando as investigações penais necessitam da assistência das autoridades de outros países, inúmeros sistemas jurídicos colocam como condição prévia a certos tipos de auxílio judiciário mútuo e à extradição que a infracção seja sancionada nos dois países.

Contudo, qualquer medida adoptada no futuro pela União Europeia deve tomar em consideração a necessidade de fazer progressivamente com que os países candidatos participem na cooperação comunitária e internacional neste domínio e evitar que se tornem refúgios para a cibercriminalidade. Deve prever-se a associação dos representantes destes países a algumas ou a todas as reuniões comunitárias sobre esta matéria.

As propostas da Comissão repartem-se da forma que se segue.

7.1. Propostas legislativas

A Comissão apresentará propostas legislativas ao abrigo do Título VI do Tratado da União Europeia no sentido de:

- aproximar as legislações dos Estados-Membros no domínio das infracções relativas à pornografia infantil. Esta iniciativa fará parte de um conjunto de propostas que incluem igualmente questões mais amplas associadas à exploração sexual das crianças e ao tráfico de seres humanos, tal como anunciado na Comunicação da Comissão relativa ao tráfico de seres humanos de Dezembro de 1998. Esta proposta estará plenamente conforme com os esforços desenvolvidos pelo Parlamento Europeu para transformar a iniciativa austríaca tendo em vista a adopção de uma decisão do Conselho relativa à pornografia infantil numa decisão-quadro que exige a aproximação das legislações. Tal é igualmente coerente com as conclusões de Tampere e a estratégia de luta contra o crime organizado definida pela União Europeia para o novo milénio. Esta iniciativa figura já no painel de avaliação elaborado para a criação de um espaço de Liberdade, de Segurança e de Justiça;

- aproximar ainda mais o direito penal material no domínio da criminalidade que utiliza as tecnologias avançadas. Tal incluirá as infracções relativas à pirataria e aos ataques por negação de serviço. A Comissão analisará igualmente a necessidade de tomar medidas contra o racismo e a xenofobia na Internet tendo em vista a apresentação de uma decisão-quadro ao abrigo do Título VI do Tratado da União Europeia que abranja as actividades racistas e xenófobas fora de linha e em linha. Finalmente, será igualmente abordado o problema das drogas ilegais na Internet;

- aplicar o princípio do reconhecimento mútuo às decisões anteriores à fase de julgamento, associadas às investigações de cibercriminalidade, e facilitar as investigações penais relativas à informática, que implicam mais de um Estado-Membro com as garantias apropriadas no que diz respeito aos direitos fundamentais. Esta proposta é compatível com as grandes linhas do programa de medidas a favor do reconhecimento mútuo, que menciona a necessidade de examinar propostas relativas à produção e à apreensão de provas.

Com base nos resultados dos trabalhos que serão realizados no futuro Fórum da União Europeia sobre esta área, a Comissão, entre outras consultas a efectuar, examinará a necessidade de tomar medidas, em especial, de natureza legislativa, sobre a questão da manutenção de dados relativos ao tráfego.

7.2. Propostas não legislativas

Prevêem-se as seguintes medidas em vários domínios:

- a Comissão criará e presidirá um Fórum da União Europeia que agrupa serviços responsáveis pela aplicação da lei, fornecedores de serviços, operadores de redes, associações de consumidores e autoridades responsáveis pela protecção dos dados, com o objectivo de intensificar a cooperação a nível comunitário, sensibilizando simultaneamente o público para os riscos que a criminalidade na Internet coloca; promover as melhores práticas em matéria de segurança informática; desenvolver instrumentos e procedimentos eficazes para lutar contra a criminalidade informática; e incentivar a evolução dos mecanismos de alerta rápida e de gestão de crises. Tratar-se-á de uma versão comunitária de fóruns semelhantes que funcionam com êxito nalguns Estados-Membros. A Comissão incentivará os Estados-Membros que ainda não dispõem destes fóruns para que os criem. A estrutura comunitária encorajará e facilitará a cooperação entre estes diversos fóruns;

- a Comissão continuará a trabalhar a favor da segurança e da confiança no quadro da iniciativa *e*Europa, do Plano de Acção Internet, do Programa TSI e do próximo Programa-quadro de IDT. Estas acções consistirão nomeadamente em facilitar a disponibilização de produtos e de serviços que apresentem um nível de segurança satisfatório e em incentivar a generalização da utilização da codificação robusta por um diálogo entre todas as partes interessadas;

- a Comissão lançará outros projectos no âmbito de programas existentes para apoiar a formação do pessoal dos serviços responsáveis pela aplicação da lei sobre as questões relativas à criminalidade que utiliza as tecnologias avançadas e a investigação a nível da criminalística informática.

- A Comissão prevê financiar medidas destinadas a melhorar o conteúdo e a utilização da base de dados das legislações nacionais dos Estados-Membros fornecida pelo estudo COMCRIME; lançará para além disso um estudo com o objectivo de ter uma visão mais exacta da natureza e da dimensão da criminalidade informática nos Estados-Membros.

7.3. Acções realizadas noutras instâncias internacionais

A Comissão continuará a desempenhar plenamente o seu papel garantindo que os Estados-Membros coordenarão a sua acção noutras instâncias internacionais em que a questão da cibercriminalidade está a ser discutida, tais como o Conselho da Europa e o G8. As iniciativas que a Comissão tomar a nível da União Europeia terão devidamente em conta os progressos alcançados noutras instâncias internacionais, embora procurando uma aproximação no âmbito da União Europeia.

* * * * *

FICHA FINANCEIRA

1. DESIGNAÇÃO DA ACÇÃO

Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade.

2. RUBRICA(S) ORÇAMENTAL(AIS) IMPLICADA(S)

B5 302

B5 820

B6 1110, B6 2111, B6 1210

3. BASE JURÍDICA

Art. 95º, 154º e 155º do Tratado CE, e art. 29º e 34º do Tratado da UE.

4. DESCRIÇÃO DA ACÇÃO

4.1. Objectivo geral da acção

A Comissão vai criar e presidir um fórum da União Europeia que agrupará responsáveis pela aplicação da lei, fornecedores de serviços Internet, operadores de redes de telecomunicações, organizações de defesa das liberdades civis, representantes dos consumidores, autoridades responsáveis pela protecção de dados e outras partes interessadas com o objectivo de reforçar a compreensão e cooperação mútuas a nível da UE. O fórum procurará sensibilizar o público para os riscos que a criminalidade na Internet coloca, promover as melhores práticas em matéria de segurança, desenvolver instrumentos e procedimentos eficazes para lutar contra a criminalidade informática, bem como incentivar a evolução dos mecanismos de alerta rápida e de gestão de crises. Os documentos pertinentes serão publicados num sítio Internet.

4.2. Período coberto pela acção e modalidades previstas para a sua renovação e prorrogação

2001 – 2002. Em 2002, será avaliada a oportunidade de prorrogação do fórum.

5. CLASSIFICAÇÃO DA DESPESA OU DA RECEITA

5.1. Despesa não obrigatória

5.2. Dotações diferenciadas

6. NATUREZA DA DESPESA OU DA RECEITA

Reuniões: despesas de viagem reembolso para peritos			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
Funcionamento do fórum, manutenção de um sítio Internet			
B6 1110	2001	JRC Deslocações em serviço	10.000 €
B6 2111	2001	JRC Dotações específicas (várias)	15.000 €
B6 1210	2001	JRC Despesas gerais	50.000 €
B6 1110	2002	JRC Deslocações em serviço	10.300 €
B6 2111	2002	JRC Dotações específicas (várias)	15.450 €
B6 1210	2002	JRC Despesas	51.500 €
Estudos sobre temas específicos			
B6 2111	2001	JRC Dotações específicas (estudos)	25.000 €
B6 2111	2002	JRC Dotações específicas (estudos)	25.750 €
Total	2001 + 2002		270.500 €

7. INCIDÊNCIA FINANCEIRA

Modo de cálculo do custo total da acção (relação entre os custos unitários e o custo total)

Reembolso das despesas de viagem para os participantes nas reuniões. Estão previstas 2 reuniões em 2001 e 3 em 2002. Serão reembolsados 15 peritos por reunião. O custo médio de reembolso por pessoa está calculado em 900 €.

Os custos, tanto em termos de pessoal como de dotações específicas, das infra-estruturas e do apoio administrativo e técnico são proporcionais ao número de efectivos afectados às actividades em causa. O orçamento para estudos é calculado com base em 2 estudos por ano, cada um com cerca de 1 pessoa/mês.

8. DISPOSIÇÕES ANTI-FRAUDE PREVISTAS

Controlos de rotina. Não se encontram previstas disposições anti-fraude adicionais.

9. ELEMENTOS DE ANÁLISE CUSTO-EFICÁCIA

9.1. Objectivos específicos e quantificáveis, população abrangida

Reforço da compreensão e cooperação mútuas a nível da UE de diferentes grupos de interesse. População abrangida: responsáveis pela aplicação da lei, fornecedores de serviços Internet, operadores de redes de telecomunicações, organizações de defesa das liberdades civis, representantes dos consumidores, autoridades responsáveis pela protecção de dados e outras partes interessadas.

9.2.Justificação da acção

O fórum é criado com o objectivo de reforçar a compreensão e cooperação mútuas a nível da UE de diferentes grupos de interesse. O fórum procura sensibilizar o público para os riscos que a criminalidade na Internet coloca, promover as melhores práticas em matéria de segurança, desenvolver instrumentos e procedimentos eficazes para lutar contra a criminalidade informática, bem como incentivar a evolução dos mecanismos de alerta rápida e de gestão de crises.

9.3.Acompanhamento e avaliação da acção

A Comissão será responsável pela organização e presidência das reuniões do fórum e participará nas discussões. A Comissão assegurará igualmente a gestão do sítio Internet criado para o efeito. A necessidade de prosseguir com as actividades do fórum em 2003 e anos seguintes será avaliada em 2002.

10. DESPESAS ADMINISTRATIVAS

As necessidades em termos de recursos humanos serão cobertas pelos efectivos existentes.

10.1. Incidência para o número de postos de trabalho

Tipos de postos de trabalho	Efectivos a atribuir para a gestão da acção		Dos quais		Duração
	Postos permanentes	Postos temporários	Por utilização dos recursos existentes na DG	Por recurso a recursos adicionais	
Funcionários ou Agentes temporários A B C	 0,05	 1,75 0,15	 1,75 0,15 0,05		Por ano durante 2 anos
Outros recursos					
Total	0,05	1,9	1,95		

10.2. Incidência financeira global dos recursos humanos

	Montantes	Modo de cálculo (2001 - 2002)
Funcionários	421.200 €	2 anos x 108.000 € x 1,95 efectivos