COMISSÃO DAS COMUNIDADES EUROPEIAS

COM(90) 314 final-SYN 287 e 288
Bruxelas, 24 de Setembro de 1990

COMUNICAÇÃO DA COMISSÃO
relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação

Proposta de
DIRECTIVA DO CONSELHO
relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais

Projecto de
RESOLUÇÃO DOS REPRESENTANTES DOS GOVERNOS DOS ESTADOS-MEMBROS DAS COMUNIDADES EUROPEIAS REUNIDOS EM CONSELHO

DECLARAÇÃO DA COMISSÃO
relativa à aplicação às instituições e organismos das Comunidades Europeias dos princípios da Directiva relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais

Proposta de
DIRECTIVA DO CONSELHO
relativa à protecção de dados pessoais e da vida privada no contexto das redes públicas digitais de telecomunicações, nomeadamente a rede digital de serviços integrados (RDSI) e as redes públicas móveis digitais

Recomendação de
DECISÃO DO CONSELHO
relativa à abertura de negociações com vista à adesão das Comunidades Europeias à Convenção do Conselho da Europa para a protecção dos indivíduos, relativamente ao tratamento automatizado de dados de carácter pessoal

Proposta de
DECISÃO DO CONSELHO
no domínio da segurança da informação

COMUNICAÇÃO DA COMISSÃO

relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação

I. INTRODUÇÃO

1. O recurso cada vez mais frequente ao tratamento de dados pessoais em todos os aspectos das actividades económicas e sociais, bem como as novas necessidades de intercâmbio de dados ligadas ao reforço da construção comunitária tornam indispensáveis a adopção na Comunidade de medidas que se destinem a assegurar a protecção das pessoas no que diz respeito aos tratamentos de dados pessoais e o reforço da segurança dos tratamentos de dados no contexto, nomeadamente, do desenvolvimento das redes abertas de telecomunicações.

2. Com efeito, no momento em que os progressos das tecnologias da informação facilitam consideravelmente o tratamento e o intercâmbio de dados de todo o tipo, a situação actual da protecção das pessoas no que diz respeito a esses tratamentos na Comunidade caracteriza-se pela diversidade das abordagens nacionais. Nos anos setenta, as preocupações relativas à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais originaram um processo legislativo em vários Estados-membros destinado a limitar e a enquadrar a utilização deste tipo de dados. Contudo, existem apenas actualmente sete Estados-membros com uma legislação específica neste domínio. Além disso, ainda que os seus objectivos sejam os mesmos, estas legislações adoptam por vezes soluções divergentes como , por exemplo, sobre a questão do âmbito de aplicação (inclusão ou não dos ficheiros manuais, protecção ou não das pessoas colectivas) ou sobre a legislação das condições prévias dos tratamentos (extensão da obrigação de notificação, informação no momento da recolha, tratamento de dados sensíveis).

3. Para além do âmbito nacional e para além da Recomendação do Conselho da OCDE relativa às linhas directrizes que regem a protecção da vida privada e os fluxos transfronteiriços de dados pessoais de 23 de Setembro de 1980, a Convenção do Conselho da Europa de 28 de Janeiro de 1981 relativa à protecção das pessoas no que diz respeito ao tratamento automatizado dos dados pessoais constitui o único instrumento de direito internacional neste domínio. Permite, no entanto, um grande número de opções para a aplicação dos princípios-quadro que definiu, tendo apenas sido ratificada por sete Estados-membros dos quais um não possui ainda legislação nacional.

4. Perante esta situação a Comunidade exprimiu já as suas preocupações. O Parlamento Europeu foi deste modo levado a adoptar, a partir de 1976, várias resoluções(1) nas quais manifesta a sua preocupação face a esta questão e convida a Comissão a preparar uma proposta de directiva destinada a harmonizar as legislações em matéria de protecção dos dados pessoais.

5. A Comissão, numa Recomendação de 29 de Julho de 1981, sublinhava que esta protecção tem o carácter de um direito fundamental e que é desejável que seja elaborada em todos os Estados-membros uma aproximação neste domínio. A Comissão recomendava igualmente aos Estados-membros que ratificassem, antes do final de 1982, a Convenção do Conselho da Europa de 28 de Janeiro de 1981 relativa à protecção das pessoas no que diz respeito ao tratamento automatizado dos dados pessoais. Todavia, especificava-se que "se num período de tempo razoável todos os Estados-membros não assinarem e ratificarem esta Convenção, a Comissão reserva-se o direito de propor ao Conselho a adopção de um acto fundamentado no Tratado CEE".

6. A diversidade das abordagens nacionais e a ausência de um sistema de protecção à escala comunitária constituem um obstáculo à realização do mercado interno. Com efeito, se os direitos fundamentais das pessoas em causa, nomeadamente, o direito à vida privada, não forem assegurados a nível comunitário, o fluxo transfronteiriço de dados poderia ser obstruído no momento em que se tornou indispensável às actividades das empresas e dos organismos de investigação, bem como à colaboração entre as Administrações dos Estados-membros no âmbito do espaço sem fronteiras previsto no artigo 8º-A do Tratado. Deste modo, recentemente, o Conselho Europeu de Estrasburgo de 8 e 9 de Dezembro de 1989, no contexto das medidas a favor da livre circu-

---

(1) J.O. nº C 100 de 3.5.1976, p.27; J.O. nº C 140 de 5.6.1979, p. 34; J.O. nº C 87 de 5.4.1982, p. 39.

lação das pessoas e da Europa dos cidadãos, sublinhou a necessidade "de velar por que as modalidades de cooperação entre administrações garantam previamente a protecção dos cidadãos face à utilização dos bancos de dados pessoais".

7. Uma abordagem comunitária em matéria de protecção das pessoas no que diz respeito ao tratamento dos dados pessoais constitui igualmente uma exigência essencial para o desenvolvimento da indústria da informática e dos serviços telemáticos com valor acrescentado. A rápida introdução de disposições harmonizadas relativas à protecção dos dados e da vida privada no contexto das redes de telecomunicações digitais revela-se indispensável para a realização do mercado interno dos equipamentos e serviços de telecomunicações.

8. A penetração da informática em todas as esferas das actividades económicas e sociais e o aparecimento de sistemas globais de comunicação que facilitam a integração de diversas actividades representam igualmente um novo desafio que obriga a criação de uma "protecção" adaptada aos riscos que podem provocar eventuais falhas técnicas ou humanas de natureza acidental ou voluntária. Uma segurança eficaz dos sistemas de informação constitui um elemento essencial para assegurar uma protecção efectiva da vida privada e para preservar a integridade das riquezas que constituem actualmente os dados registados e transmitidos electronicamente. As políticas e os programas comunitários para o desenvolvimento das indústrias da informação e das telecomunicações e a realização do mercado interno ameaçam ser seriamente entravados caso não seja adoptada uma política activa de criação, de desenvolvimento e de promoção de normas de segurança para os sitemas de informação. As telecomunicações permitem actualmente os intercâmbios de dados à escala planetária, devendo essa política, por conseguinte, tomar em consideração esta dimensão. É, além disso, essencial que as políticas nacionais em matéria de segurança da informação se não transformem num obstáculo à promoção do desenvolvimento harmonioso da Comunidade e às relações com os países terceiros.

II A ACÇÃO PROPOSTA

9. A abordagem proposta tem por objectivo assegurar um alto nível de protecção através de um sistema comunitário de protecção que assenta num conjunto de medidas complementares entre si.

A Um alto nível de protecção

10. Tendo as legislações nacionais por objectivo garantir os direitos fundamentais das pessoas, nomeadamente o direito à vida privada, e tendo a própria Comunidade exprimido o seu empenho nos direitos fundamentais, em especial, no terceiro parágrafo do Preâmbulo do Acto Único Europeu, a acção da Comunidade não deve ter por efeito diminuir a protecção mas, pelo contrário, assegurar um alto nível de protecção no conjunto da Comunidade. Através de uma acção comunitária é possível garantir um alto nível de protecção equivalente em todos os Estados-membros da Comunidade afastando, através da mesma acção, obstáculos à criação do mercado interno em conformidade com o artigo 100Ω-A.

11. Como complemento da aproximação a um nível elevado dos direitos reconhecidos às pessoas, o lançamento de uma política activa em matéria de segurança dos sitemas de informação revela-se indispensável. A segurança dos sitemas de informação é vital tanto para as pessoas como para o comércio, a indústria e as administrações públicas. O desafio principal é garantir uma segurança eficaz e prática da informação detida electronicamente, evitando a formação de novos obstáculos técnicos entre Estados-membros ou face a países terceiros. Esta exigência obriga ao exame a nível comunitário das necessidades e das opções possíveis em colaboração estreita com os intervenientes do sector e os Estados-membros.

B Uma abordagem global

12. Para estabelecer na Comunidade um sistema de protecção das pessoas no que diz respeito ao tratamento dos dados pessoais, é necessário prever várias medidas que permitam abranger os diversos aspectos desta questão.

13. A nível interno , para além de uma directiva-quadro relativa à aproximação de certas disposições legislativas, regulamentares e administrativas dos Estados-membros respeitantes à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais (directiva geral), que constitui o elemento central do sistema de protecção, é proposto um conjunto de outras medidas complementares destinado a assegurar uma protecção o mais

completa possível. Cada uma das medidas propostas é adaptada a uma situação específica, procedendo todas dos mesmos princípios de protecção que se encontram na directiva geral. Deste modo, uma resolução dos representantes dos Governos dos Estados-membros reunidos no seio do Conselho e uma declaração da Comissão têm por objectivo tornar aplicáveis os princípios da directiva aos ficheiros que não estão abrangidos por esta. Do mesmo modo, é necessária uma directiva sectorial no contexto das redes de telecomunicações digitais públicas. Finalmente, a segurança dos sistemas de informação necessita de um plano de acção comunitária.

14. A nível externo , a Comunidade Europeia deve promover junto dos seus parceiros a aplicação de disposições de protecção adequadas e apoiar os esforços envidados pelo Conselho da Europa nesta matéria. É desejável neste contexto, nomeadamente, que a Comunidade enceté negociações tendo em vista a sua adesão à Convenção 108 do Conselho da Europa.

Estas propostas não podem ser dissociadas umas das outras sem prejudicar a homogeneidade e a corência do sistema de protecção proposto.

C Apresentação das propostas

15. A proposta de directiva geral tem por objectivo estabelecer uma protecção equivalente de alto nível em todos os Estados-membros da Comunidade a fim de eliminar os obstáculos aos intercâmbios dos dados necessários ao funcionamento do mercado interno. Para esse efeito, os princípios enunciados no projecto de proposta de directiva devem ser garantidos pelos Estados-membros. Estes princípios referem-se, nomeadamente, às condições em que um tratamento de dados pessoais é legítimo; aos direitos da pessoa em causa (direito à informação, direito de acesso, direito de rectificação, direito de oposição, etc.), às qualidades que os dados devem possuir (devem ser exactos, recolhidos lealmente, registados com finalidades determinadas e legítimas, etc.), à criação de um Grupo de protecção dos dados pessoais que assistirá a Comissão nas questões de protecção dos dados. O projecto de proposta de directiva abrange o sector privado e o sector público, cujas actividades relevem do âmbito de aplicação do direito comunitário. Uma vez que qualquer pessoa beneficiará em cada Estado-membro de uma protecção equivalente de alto nível no que diz respeito ao tratamento de

dados pessoais, os Estados-membros devem deixar de colocar restrições à circulação destes últimos na Comunidade com base na protecção da pessoa em causa.

16. O projecto de resolução dos representantes dos Estados-membros das Comunidades Europeias reunidos no seio do Conselho tem por objectivo alargar a cobertura dos princípios da directiva geral aos ficheiros do sector público por ela não abrangidos, ou seja, os ficheiros das administrações cujas actividades não relevam do âmbito de aplicação do direito comunitário. Com efeito, por uma questão de coerência, não seria desejável que todos os ficheiros das administrações, mesmo os que não estão abrangidos pela directiva geral, estivessem sujeitos aos mesmos princípios de protecção. Para este efeito, os Estados-membros deveriam comprometer-se a dar início aos processos legislativos nacionais necessários.

17. A declaração da Comissão relativa à aplicação às instituições e organismos da Comunidade das disposições da directiva geral manifesta o desejo da Comissão de que os princípios da directiva se apliquem às instituições e organismos da Comunidade. Prevê, relativamente a este ponto, que a Comissão tome e proponha as medidas necessárias e indica que, na pendência, aplique as disposições da directiva aos seus próprios ficheiros.

18. A proposta de directiva do Conselho relativa à protecção dos dados pessoais e da vida privada no contexto das redes de telecomunicações digitais públicas e, em especial, da rede digital de serviços integrados (RDSI) e das redes digitais móveis públicas, completa a directiva geral aplicando os princípios gerais da protecção dos dados às necessidades específicas das novas redes de telecomunicações. A directiva tem por objectivo garantir aos utilizadores das telecomunicações em todos os Estados-membros um nível básico de protecção através de medidas que devem ser integradas nos serviços oferecidos pelas novas redes. O Conselho e o Parlamento Europeu acentuaram em várias ocasiões a importância de medidas apropriadas para assegurar a protecção dos dados e da vida privada relativamente aos futuros desenvolvimentos das telecomunicações e, nomeadamente, da RDSI [1]. Esta preocupação foi veementemente expressa pelos Comissários dos Estados-membros encarregados da protecção dos dados no seu encontro

---

(1) J.O. nº C 257 de 4.10.1988, p.1; J.O. nº C 196 de 1.8.1989, p.4;
J.O. nº C 7 de 12.1.1987, p.334; J.O. nº C 12 de 16.1.1989, p. 66;
J.O. nº C 12 de 16.1.1989, p.69.

anual em Berlim em Agosto de 1989.

19. A recomendação de decisão do Conselho relativa à adesão da Comunidade Europeia à Convenção do Conselho da Europa relativa à protecção das pessoas no que diz respeito ao tratamento automatizado dos dados pessoais constitui um dos aspectos externos da abordagem da Comunidade em matéria de protecção dos dados pessoais. A adesão à Convenção assegurará, com efeito, nas relações entre a Comunidade e os países terceiros parte, a protecção das pessoas em causa e a circulação transfronteiriça dos dados pessoais.

20. A proposta de decisão do Conselho relativa à adopção de um plano de acção de dois anos em matéria de segurança dos sistemas de informação completará o dispositivo destinado a reforçar os direitos das pessoas no que diz respeito ao tratamento dos dados pessoais. A segurança da informação, ou seja, a protecção dos dados conservados, tratados e transmitidos electronicamente contra as ameaças de qualquer natureza (acidentais ou voluntárias) revela-se essencial para o exercício efectivo dos direitos das pessoas no que diz respeito aos tratamentos de dados pessoais. Constitui mais em geral uma exigência primordial para a protecção dos bens e das pessoas que, no contexto da instalação das redes de telecomunicações abertas, exige do desenvolvimento de uma estratégia global, das acções concertadas a nível comunitário no domínio das tecnologias, das normas e dos processos de homologação e de ensaio, bem como dos desenvolvimentos tecnológicos que implicam uma colaboração no estádio da investigação e do desenvolvimento pré-competitivo.

21. O plano de acção proposto prevê o desenvolvimento de um enquadramento estratégico para a segurança dos sistemas de informação, a análise das necessidades em matéria de segurança, a elaboração de soluções para determinadas necessidades prioritárias, a elaboração de especificações, normas e ensaios de validação, a integração dos desenvolvimentos tecnológicos e operacionais em matéria de segurança dos sitemas de informação num quadro estratégico geral e a integração de certas funções de segurança nos sistemas de informação.

Proposta de SYN 287

DIRECTIVA DO CONSELHO

relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais.

TABLE DES MATIERES

Résumé

Exposé des motifs

I. Introduction

II. La nécessité d'une protection dans la Communauté

- La disparité des législations nationales et l'absence de protection équivalente

- Conséquences de cette situation pour la Communauté

III. L'approche adoptée

- Une protection équivalente dans la Communauté

- Un haut niveau de protection

IV. Examen des dispositions

Proposition de directive

Résumé

Cette proposition de directive a pour objet d'établir une protection équivalente de haut niveau dans tous les Etats membres de la Communauté afin d'éliminer les obstacles aux échanges des données nécessaires au fonctionnement du marché intérieur. Pour cela, les principes énoncés dans le projet de proposition de directive doivent être garantis par les Etats membres. Ces principes sont relatifs notamment aux conditions dans lesquelles un traitement de données à caractère personnel est légitime, aux droits de la personne concernée (droit à l'information, droit d'accès, droit de rectification, droit d'opposition, etc...), aux qualités que doivent avoir les données (elles doivent être exactes, collectées loyalement, enregistrées pour des finalités déterminées et légitimes, etc...), à la création d'un Groupe de protection des données à caractère personnel qui conseille la Commission sur les questions de protection des données. Le projet de proposition de directive couvre le secteur privé ainsi que le secteur public dont les activités relèvent du champ d'application du droit communautaire. Puisque toute personne bénéficiera dans chaque Etat membre d'une protection équivalente de haut niveau à l'égard du traitement de données à caractère personnel, les Etats membres ne pourront plus opposer des restrictions à la circulation de ces dernières dans la Communauté fondées sur la protection de la personne concernée.

Exposé des motifs

I. INTRODUCTION

Les préoccupations relatives à la protection des personnes à l'égard du traitement des données à caractère personnel, exprimées depuis ces quinze dernières années, sont suscitées à la fois par les possibilités offertes par les progrès techniques dans le domaine du traitement de l'information et par le recours de plus en plus fréquent au traitement de données à caractère personnel dans une multitude de domaines. Ces préoccupations se sont manifestées dans différents cadres et ont animé un processus législatif dans plusieurs Etats membres. Au-delà du cadre national, la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel est, actuellement, le seul instrument de droit international dans ce domaine. L'OCDE a établi des lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel dans une recommandation du 23 septembre 1980 et les Nations Unies sont également en train de le faire.

Ces préoccupations ont été aussi exprimées dans le cadre de la Communauté. Le Parlement européen a été ainsi amené à adopter dès 1976 plusieurs résolutions(1) dans lesquelles il manifeste son inquiétude à l'égard de cette question et invite la Commission à préparer une proposition de directive visant à harmoniser les législations en matière de protection des données à caractère personnel.

---

(1) JO n° C 100 du 3. 5. 1976, p. 27; JO n° C 140 du 5. 6. 1979, p. 34; JO n° C 87 du 5. 4. 1982, P. 39.

La Commission, dans une recommandation du 29 juillet 1981, soulignait que cette protection a le caractère d'un droit fondamental et qu'il est souhaitable qu'un rapprochement dans ce domaine soit élaboré dans tous les Etats membres. Elle recommandait également aux Etats membres de ratifier, avant la fin de l'année 1982, la Convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Toutefois, il était précisé que "si dans un laps de temps raisonnable tous les Etats membres ne devaient pas signer et ratifier cette convention, la Commission se réserve le droit de proposer au Conseil d'arrêter un acte fondé sur le traité CEE".

Le Conseil Européen de Strasbourg des 8 et 9 décembre 1989, dans le contexte des mesures en faveur de la libre circulation des personnes et de l'Europe des citoyens, a souligné la nécessité "de veiller à ce que les modalités de la coopération entreadministrations garantissent préalablement la protection des citoyens face à l'utilisation des banques de données personnelles".

En dehors de ces prises de positions sur la nécessité d'une protection générale, il faut noter que cette préoccupation s'est aussi manifestée dans le cadre d'actions spécifiques ou sectorielles de la Communauté, en particulier dans le domaine des nouvelles technologies de l'information.

Au regard de la situation actuelle dans le domaine du traitement des données à caractère personnel et des exigences de la construction communautaire, une directive visant à assurer une protection des personnes à l'égard de ce type de traitements devient indispensable.

II. LA NECESSITE D'UNE PROTECTION DANS LA COMMUNAUTE

La disparité des législations nationales et l'absence de protection équivalente dans la Communauté

La protection des personnes à l'égard des données à caractère personnel fait l'objet d'une diversité d'approches dans les Etats membres. Cette

diversité résulte, à la fois, du fait que certains Etats membres n'ont pas de législation spécifique dans ce domaine et, lorsqu'ils en ont, de leur contenu différent.

Actuellement, sept Etats membres disposent de législations spécifiques (Allemagne, Danemark, France, Irlande, Luxembourg, Pays-Bas, Royaume-Uni). Des travaux sont en cours dans certains autres Etats membres.

Si l'objectif de ces législations nationales est le même, assurer la protection de la personne concernée, elles adoptent, toutefois, des solutions différentes en raison de la multiplicité des options possibles pour garantir une telle protection. Ainsi, par exemple, la couverture des fichiers manuels, la protection des personnes morales, les procédures préalables à la création de fichiers, l'étendue de l'obligation de notification, l'information lors de la collecte des données, le traitement de données sensibles, le transfert vers d'autres pays, sont autant de questions qui peuvent faire l'objet d'une approche différente. En outre, les développements de la technologie peuvent conduire les Etats à réagir différemment et à accentuer ainsi cette disparité.

La Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel n'a pas permis de limiter cette disparité dans la mesure où, d'une part, elle laisse ouvert un grand nombre d'options pour la mise en oeuvre des principes de base qu'elle définie et, d'autre part, elle n'a été ratifiée que par sept Etats membres (Allemagne, Danemark, Espagne, France, Irlande, Luxembourg, Royaume-Uni) dont un (Espagne) qui n'a toujours pas de législation interne. La recommandation de la Commission du 29 juillet 1981 invitant les Etats membres de la Communauté à ratifier la convention du Conseil de l'Europe n'a pas modifié cette situation.

En raison de la disparité des approches nationales, la protection des personnes à l'égard des traitements de données à caractère personnel n'est pas équivalente dans tous les Etats membres, le niveau de protection pouvant en effet varier d'un Etat à un autre.

Conséquences de cette situation pour la Communauté

Dans la Communauté, une telle situation soulève trois types de difficultés:

- L'absence de législations nationales spécifiques ou leurs lacunes ne correspondent pas à l'attachement de la Communauté au respect des droits fondamentaux tel qu'il a été souligné dans la Déclaration commune du Parlement européen, du Conseil et de la Commission sur les droits fondamentaux du 5 avril 1977 et dans le troisième paragraphe du préambule de l'Acte unique européen. Au delà de ces textes, en droit communautaire, le respect des droits fondamentaux fait partie intégrante des principes généraux du droit dont la Cour de Justice des Communautés européennes assure le respect.

- La circulation des données à caractère personnel, lorsqu'elle se fait dans le respect des droits de la personne concernée, apparaît comme une nécessité dans le cadre de l'établissement et du fonctionnement du marché intérieur. En effet, compte tenu des développements techniques dans le domaine du traitement de l'information, notamment de la mise en place des réseaux de télécommunication numériques dans la Comunauté, la dimension transfrontière des flux de données apparaît à trois niveaux:
  . L'utilisation des données à caractère personnel intervient à de nombreux stades des activités économiques. L'exercice de la libre circulation des marchandises, des personnes, des services et des capitaux nécessite que des données à caractère personnel puissent être transmises entre les opérateurs ayant des activités transfrontières.
  . Dans le processus d'intégration communautaire, en particulier dans le contexte de l'abolition des frontières, la coopération et la collaboration entre les administrations nationales sont amenées à s'intensifier. Les administrations nationales sont appelées ainsi à remplir des tâches qui relèvent d'une administration d'un autre Etat membre. Dans ce contexte la circulation des données devient une condition indispensable du processus de coopération. Ainsi, les devoirs de collaboration ou d'information qui seront imposés aux administrations par le droit communautaire nécessitent que, parallélement, la protection des personnes à l'égard des personnes concernées soit pleinement assurée.

. Les échanges de données sont également nécessaires à la coopération scientifique.

Ce besoin de permettre la circulation des données entre Etats membres se heurte actuellement à la disparité des approches nationales en matière de protection des personnes à l'égard des traitements de données à caractère personnel. Cette disparité peut, en effet, conduire un Etat membre à opposer des entraves à la circulation des données en invoquant l'absence ou l'insuffisance de la protection dans l'Etat de provenance ou de destination.

- Cette disparité pourrait, également, dans certains cas, fausser le jeu de la concurrence entre les opérateurs privés selon le degré de contraintes auxquelles ils sont soumis dans leur pays.

III. L'APPROCHE ADOPTEE

Une protection équivalente dans la Communauté

Afin d'assurer à toute personne résidant dans la Communauté une protection à l'égard des traitements de données à caractère personnel et de permettre la circulation de ce type de données entre les Etats membres, il est nécessaire d'établir un niveau de protection équivalent dans l'ensemble de la Communauté. Pour cela un rapprochement des législations s'avère indispensable. Le programme de travail de la Commission pour 1990 mentionne d'ailleurs la protection des données comme dossier prioritaire dans le cadre de l'achèvement du marché intérieur(1).

A cet égard, l'article 100 A du Traité fournit la base juridique appropriée dans la mesure où une protection équivalente de haut niveau est indispensable à la réalisation du marché intérieur. L'achèvement et le fonctionnement du marché intérieur, définis dans l'article 8 A comme "un espace sans frontières intérieures dans lequel la libre circulation des marchandises, des personnes, des services,et des capitaux est assurée selon les dispositions du présent Traité", nécessitent, pour les raisons déjà soulignées, un rapprochement des législations dans ce domaine.

---

(1) Bull. CE Suppl. 1/90, page 18, 26 et 28.

En élaborant la présente proposition, la Commission a tenu compte des exigences de l'article 8C du traité CEE et a conclu que des dispositions spéciales ou des dérogations ne paraissent pas utiles ou justifiées au stade actuel. De même, la Commission a étudié le problème du niveau élevé de protection de la santé, de la sécurité, de l'environnement et des consommateurs requis par l'article 100A paragraphe 3 du traité CEE.

Un haut niveau de protection

L'objet des législations nationales dans ce domaine étant d'assurer une protection des droits fondamentaux, notamment le droit à la vie privée, un rapprochement de ces législations doit avoir pour objectif de garantir un haut niveau de protection. En dehors des adaptations inhérentes à tout rapprochement de législations, celui-ci ne doit pas avoir pour conséquence de diminuer le niveau de protection déjà assuré dans les Etats membres.

Les principes généraux énoncés dans la Convention du Conseil de l'Europe sont une référence à prendre en compte car ils constituent déjà une base commune pour les pays l'ayant ratifiée. Ainsi tout en adoptant des solutions compatibles avec celles de la Convention, la directive complète ces principes généraux afin d'établir une protection équivalente de haut niveau.

Un haut niveau de protection nécessite que la protection garantie par la directive ait une très large couverture et que soient visées toutes les situations dans lesquelles le traitement de données à caractère personnel comporte un risque pour les personnes concernées. Ceci explique que la directive vise aussi bien les fichiers manuels que automatisés, ainsi que les fichiers du secteur public et ceux du secteur privé.

Les principes de la directive, notamment ceux relatifs à la légitimité des traitements, à la communication des données à des tiers, aux procédures de notifications, aux droits de la personne concernée, aux qualités des données, visent à assurer un haut niveau de protection en prenant comme référence les diverses solutions adoptées dans les législations nationales.

De même, les moyens d'assurer, au-delà des mécanismes habituels de contrôle de l'application du droit communautaire, une application effective des dispositions de la directive ont fait l'objet d'une attention particulière. Ainsi, les dispositions relatives à la responsabilité et à l'établissement d'un Groupe de protection des données à caractère personnel procèdent de ce souci.

Les principes de la directive pourront, le cas échéant, être complétés. La directive prévoit à cet effet dans plusieurs dispositions que les Etats membres peuvent apporter des précisions pour les fichiers qui sont soumis à leur législation. Des mesures complémentaires pourront être également nécessaires pour l'application de certains principes généraux à des secteurs présentant des spécificités importantes.

IV. EXAMEN DES DISPOSITIONS

CHAPITRE I

Dispositions générales

Article premier

Objet de la directive

Cet article prévoit que les Etats membres ont l'obligation d'assurer la protection des personnes à l'égard des traitements de données à caractère personnel en appliquant les dispositions de la directive. Etant donné que, en vertu de la présente directive, la protection est assurée selon les mêmes principes dans tous les Etats membres et est donc équivalente, ceux-ci ne peuvent plus restreindre, pour les domaines couverts par la directive, la circulation des données pour des motifs relatifs à la protection de la personne concernée. La protection des personnes et la circulation des données ne sont toutefois garanties en vertu de la

directive que pour les domaines couverts par celle-ci. Ainsi, les fichiers détenus à des fins privées ou ceux des associations sans but lucratif ne peuvent pas donner lieu à l'application des dispositions du présent article dans la mesure où l'article 3 paragraphe 2 les exclut du champ d'application de la directive.

Article 2

Définitions

Cet article a pour objet de définir les principales notions utilisées dans la directive. Les définitions reprennent celles de la convention 108 du Conseil de l'Europe en y apportant toutefois les adaptations et les précisions nécessaires pour garantir une protection équivalente de haut niveau dans la Communauté.

a) "Donnée à caractère personnel". Comme dans la convention 108, une définition large est adoptée afin de couvrir toutes les informations qui peuvent être reliées à une personne. En effet, selon la finalité de son utilisation toute donnée relative à une personne, même apparemment inoffensive, peut avoir un caractère sensible (comme une simple adresse postale par exemple). Afin d'éviter que des moyens d'identification indirecte permettent de contourner cette définition, il est précisé qu'est considérée comme identifiable une personne qui peut etre identifiée par référence à un numéro ou une information de ce type.

b) "Rendre anonyme". Cette notion a pour objet de permettre l'exclusion des données qui ne sont plus identifiables de l'application de certaines dispositions de la directive. Une donnée peut être considérée comme rendue anonyme même si théoriquement elle pourrait être de nouveau personnalisée par des moyens techniques et financiers disproportionnés.

c) "Fichier de données à caractère personnel". La définition est fondée sur le critère de la possibilité d'accès aux données à caractère personnel, soit au moyen d'un traitement manuel consistant en une collection de données structurées, soit au moyen d'un traitement automatisé qui peut permettre le regroupement de données disséminées ou d'extraire des données d'un texte intégral selon un mode de consultation qui correspond à celui d'un fichier.
La définition couvre ainsi les fichiers mécanographiques et manuels structurés. Les dossiers individuels, en particulier les dossiers administratifs, qui ne contiennent pas une collection structurée de données à caractère personnel ne sont pas visés en raison des législations spécifiques et diverses les concernant dans les Etats membres.

d) "Traitement". En énumérant les principales actions de traitement, cette définition adapte celle de la convention au champ d'application plus large de la notion de fichier. Les opérations d'interconnexion des données sont visées car elles permettent d'élaborer de nouvelles données (profil électronique par exemple). La référence au verrouillage concerne le cas des données dont l'accès est bloqué au delà des mesures de sécurité normales sans toutefois que cela équivaille à leur effacement.

e) "Responsable du fichier". La notion de "maître du fichier" de la convention est adaptée de deux manières : d'une part, en faisant référence au droit communautaire afin de viser le cas où des directives spécifiques contiennent des dispositions matérielles relatives à la protection des données à caractère personnel; d'autre part, en précisant que celui qui autorise la consultation, notamment en cas d'interrogation directe, est le responsable du fichier.

f) "Autorité de contrôle". Cette définition souligne que l'autorité doit être indépendante et renvoie à l'article 26 qui précise les fonctions de l'autorité de contrôle.

g) et h)

"Secteur public" et "secteur privé". Les définitions du secteur public et du secteur privé se justifient dans la directive car certaines de ses dispositions sont spécifiques à l'un ou l'autre des secteurs (chapitre II et III relatifs à la légitimité des traitements de données à caractère personnel dans le secteur public et dans le secteur privé). Ces définitions se fondent sur la nature du service fourni par l'organisme concerné, quel que soit le statut privé ou public de celui-ci. Selon qu'il exerce des activités commerciales ou des missions de service public, l'organisme devra appliquer les règles spécifiques au secteur privé ou au secteur public.

Article 3

Champ d'application

La directive s'applique à tous les fichiers dont les responsables relèvent du secteur privé ou du secteur public. En effet, pour ce dernier, l'accomplissement de nombreuses activités administratives nécessite, en vertu du droit communautaire, une coopération entre les administrations des Etats membres. Toutefois ne sont pas visés les fichiers du secteur public dont les activités ne relèvent pas du champ d'application du droit communautaire. Ceci concerne le cas des fichiers utilisés exclusivement pour des activités ne pouvant être rattachées au champ d'application du droit communautaire (comme les services secrets).

Le paragraphe 2 prévoit deux exclusions qui se justifient par le fait que des atteintes à la vie privée sont peu susceptibles de se produire soit parce qu'il s'agit d'une utilisation de données à des fins totalement privées, comme l'agenda électronique personnel par exemple, soit parce qu'il s'agit des registres de membres d'une association dont leur consentement à y figurer peut être présumé de leur simple adhésion et parce que les informations contenues dans ce registre ne sont pas transmises à des tiers.

Article 4

Droit applicable

Cet article fixe les critères de rattachement qui déterminent l'application dans chaque Etat membre des dispositons de la présente directive.
Le choix des critères, dans le paragraphe 1, est animé par le souci d'éviter que la personne concernée ne soit soustraite de toute protection, en particulier du fait d'un contournement de législation. Ainsi le critère factuel du lieu de localisation du fichier a été adopté. A cet égard, chaque partie d'un fichier multilocalisé ou réparti dans plusieurs Etats membres doit être considérée comme un fichier à part entière.

Le même souci de protection de la personne concernée en cas de délocalisation est à l'origine d'une disposition qui impose à l'utilisateur qui consulte un fichier localisé dans un pays tiers à partir d'un terminal localisé dans un Etat membre de respecter les dispositions de la directive relatives à la légitimité des traitements, à l'information de la personne concernée en cas de communication des données, aux données sensibles, à la sécurité des données et à la responsabilité. Cette obligation s'applique en dehors des cas où une telle utilisation n'est que sporadique.

Compte tenu de la facilité de déplacement des fichiers, le déplacement temporaire d'un fichier ne constitue pas un changement de localisation. Le déplacement de supports dans lesquels sont enregistrées les données ne doit pas provoquer de nouvelles formalités par rapport à celles qui ont été satisfaites dans l'Etat de localisation permanente.

Cet article a également pour objectif d'éviter les cas de cumul des lois applicables.

CHAPITRE II

Légitimité du traitement dans le secteur public

Les données à caractère personnel ne peuvent faire l'objet d'un traitement que si celui-ci est légitime. Ce chapitre, comme le chapitre III, précise les conditions dans lesquelles un traitement est légitime. La source de la légitimité se trouve, selon les cas, dans le consentement de la personne concernée, dans une disposition de la directive ou de droit communautaire, dans un acte légal national.

Article 5

Principes

Cet article prévoit que l'établissement d'un fichier du secteur public et tout autre traitement de donnée ne sont légitimes que si cela est nécessaire pour l'exécution des missions de l'autorité publique responsable du fichier.

Quatre cas sont prévus où le traitement de donnée peut être effectué pour une autre finalité que celle pour laquelle le fichier a été établi: s'il y a consentement de la personne concernée, si le traitement est fondé sur une base légale, si, après avoir fait une balance des intérêts en présence, il apparaît qu'un intérêt légitime de la personne concernée ne s'y oppose pas, et, enfin, en cas de menace imminente pour l'ordre public ou une atteinte sérieuse au droit d'autrui.

Ces principes ne concernent pas le cas spécifique de la communication des données à des tiers qui fait l'objet des dispositions de l'article 6.

Article 6

Traitement dans le secteur public ayant pour objet la communication de données à caractère personnel,

Une disposition spécifique pour la communication des données à des tiers est nécessaire dans la mesure où ce type de traitement fait courir le plus grand risque pour la personne concernée. Le paragraphe prévoit deux cas dans lesquels les données peuvent être communiquées à des tiers selon que le destinataire relève du secteur public ou du secteur privé. Dans le premier cas la communication doit être nécessaire à l'exercice des fonctions de l'administration qui demande ou qui communique ces données, dans le second, une balance des intérêts doit être faite afin de déterminer si le demandeur justifie d'un intérêt légitime et si l'intérêt de la personne concernée ne prévaut pas.

Les Etats membres ont la possibilité de préciser dans leur législation les conditions de légitimité de la communication dans les limites des deux principes énoncés ci-dessus. Les précisions pourront consister, par exemple, à définir dans certains domaines dans quel cas l'intérêt de la personne concernée prévaut.

Afin de s'assurer que la possibilité de communication au secteur privé ne se fasse pas au détriment des intérêts de la personne concernée, une procédure d'information de celle-ci est prévue. Toutefois, une dérogation à cette obligation est possible si elle est autorisée par l'autorité de contrôle. Celle-ci peut l'assortir de conditions ou décider d'informer elle-même la personne concernée.

Article 7

Obligation de notification à l'autorité de contrôle

L'obligation, prévue dans cet article, de notification dans un registre tenu par l'autorité de contrôle se limite aux fichiers du secteur public dont les données sont susceptibles d'être communiquées. Cette solution vise à permettre le minimum de transparence nécessaire à l'exercice des droits de la personne concernée tout en allégeant les formalités préalables qui

pourraient constituer une charge très lourde pour l'autorité de contrôle, notamment en raison de la notion large de fichier. Les Etats membres ont la possibilité, toutefois, d'étendre l'obligation de notification à d'autres fichiers du secteur public.

CHAPITRE III

Légitimité du traitement dans le secteur privé

Article 8

Principes

La légitimité du traitement de données à caractère personnel dans le secteur privé peut être fondée sur le consentement de la personne concernée. Ce consentement doit être exprimé en conformité avec les dispositions des articles 12 relatif au consentement informé et 13 relatif à l'information lors de la collecte.

En l'absence de consentement de la personne concernée, la légitimité du traitement peut être fondée sur l'existence d'une relation de type contractuel entre le responsable du fichier et la personne concernée dans la mesure où le traitement est nécessaire à la réalisation du contrat (par exemple, traitement des commandes ou facturation).

La légitimité du traitement peut être fondée également sur le fait que les données proviennent de sources généralement accessibles au public (annuaires accessibles au public) dans la mesure où le traitement est uniquement destiné à la correspondance.

Enfin, la légitimité du traitement peut être fondée sur une balance d'intérêts qui révèle que le responsable du fichier a un intérêt légitime et que la personne concernée n'a pas un intérêt qui prévaut.

La communication de données n'est légitime que si elle est compatible avec la finalité du fichier telle qu'elle doit être notifiée (article 11 § 2), et respectée lors de l'enregistrement des données (article 16 § 1 b). En cas de communication le responsable du fichier est soumis en outre à une obligation d'informer la personne concernée décrite dans les articles 9 et 10. Les Etats membres ont la possibilité de préciser dans leur législation les conditions de légitimité dans les limites des principes énoncés ci-dessus. Les précisions pourront consister, par exemple, à définir dans certains domaines dans quel cas l'intérêt de la personne concernée prévaut.

Article 9

Obligation d'information de la personne concernée

Afin de permettre à la personne concernée d'exercer ses droits, le paragraphe premier oblige le responsable du fichier d'informer la personne concernée que des données la concernant ont été communiquées. La personne concernée peut ainsi exercer son droit d'accès et s'opposer à la poursuite du traitement en cause. L'obligation d'informer la personne concernée ne s'applique pas dans le cas où les données proviennent de sources généralement accéssibles au public et leur traitement est uniquement destiné à la correspondance.

Article 10

Exceptions particulières à l'obligation d'informer la personne concernée

Cet article donne la possibilité aux Etats membres de prévoir dans leur législation que dans les cas où l'information de la personne concernée se heurte à des difficultés pratiques majeures ou à des intérêts légitimes prédominant du responsable du fichier ou à un intérêt similaire d'un tiers, l'autorité de contrôle peut, dans les limites de la législation qui l'y autorise, autoriser sur demande du responsable du fichier une dérogation à l'obligation d'informer la personne concernée. L'autorité de contrôle peut préciser, dans les limites de la législation qui l'y autorise, les conditions de la dérogation et décider d'informer elle-même la personne concernée.

Le cas de difficultés pratiques majeures vise par exemple les données relatives à des personnes dont l'adresse personnelle n'est pas connue.

Article 11

Obligation de notification à l'autorité de contrôle

Pour les mêmes raisons que celles qui ont motivé l'obligation de notification dans le secteur public (article 7), l'obligation de notification dans le secteur privé ne s'applique pas aux fichiers dont les données ne sont pas destinées à être communiquées ou qui proviennent de sources généralement accessibles au public. La notification doit être mise à jour si le fichier change de finalité.

Les informations à notifier doivent donner les éléments nécessaires au contrôle du respect des dispositions de la présente directive (au moins le nom et l'adresse du responsable du fichier, la finalité du fichier, une description des types de données qu'il contient, les tiers auxquels les données sont susceptibles d'être communiquées et une description des mesures de sécurité). Les Etats membres peuvent étendre le champ d'application de l'obligation de notification.

CHAPITRE IV

Droits de la personne concernée

Article 12

Le consentement informé

Cet article énonce les règles à respecter pour que le consentement de la personne concernée pour un traitement de données la concernant, aussi bien dans le secteur public que privé, soit légalement valable.

Le consentement de la personne concernée pour le traitement des données la concernant est un élément important de la licéité du traitement de données à caractère personnel par le responsable du fichier. Le terme "consentement" utilisé à l'article 12 désigne un "consentement informé". Pour permettre à la personne concernée d'apprécier les risques et les avantages du traitement des données la concernant et d'exercer ses droits en vertu de l'article 14 du projet de directive (rectification effacement verrouillage), le responsable du fichier doit communiquer à la personne concernée les informations dont celle-ci a besoin pour prendre une décision, par exemple le nom et l'adresse du responsable, l'objet du fichier, les données enregistrées, etc.

En ce qui concerne la forme du consentement, le projet de directive ne prévoit pas que le consentement de la personne concernée doit être donné par écrit. Cependant, l'accord doit être exprès.

Le consentement de la personne concernée doit être spécifique, c'est-à-dire qu'il doit avoir trait au traitement des données relatives à la personne concernée par un responsable déterminé d'un fichier et pour des finalités déterminées. En outre, l'accord doit préciser les types de données traitées, les formes de traitement et les destinataires éventuels en cas de transfert de données à des tiers.

En vertu de l'article 12 alinéa c), la personne concernée a le droit de retirer son consentement à tout moment. La révocation n'a toutefois pas d'effets rétroactifs, car sinon un traitement de données à caractère personnel précédemment licite deviendrait illégal rétroactivement.

Article 13

L'information de la personne concernée lors de la collecte

Une bonne protection des données passe par l'information complète de la personne concernée sur le traitement des données à caractère personnel la

concernant, non seulement lorsque ces données sont déjà enregistrées et traitées dans un fichier, mais à un stade antérieur au traitement des données, c'est-à-dire lors de la collecte des informations à caractère personnel.

En vertu de l'article 16 paragraphe 1 alinéa a), les données doivent être rassemblées loyalement et licitement. Cette règle est précisée à l'article 13 dans le cas où les données sont obtenues auprès de la personne concernée elle-même.

Pour que la collecte des données soit loyale et licite, il faut que la personne concernée puisse décider de communiquer ou de ne pas communiquer les données la concernant en s'appuyant sur des informations fiables en ce qui concerne les finalités du traitement, l'identité du responsable du fichier et le caractère légalement obligatoire ou simplement facultatif de la communication des données. Pour que la personne concernée puisse faire valoir ses droits en vertu de l'article 14 du projet de directive et contrôler effectivement l'utilisation des données la concernant, elle doit également être informée au sujet de son droit d'accès et de rectification et des destinataires des données.

L'article 13 paragraphe 1 fait obligation aux Etats membres de prévoir, dans leur législation nationale relative à la protection des données, que la personne concernée a le droit d'obtenir ces informations.

Fréquemment, les personnes qui assurent la collecte de données ne sont pas les responsables du fichier dans lequel les données seront ultérieurement enregistrées et traitées. Pour que la personne concernée puisse faire valoir ses droits auprès de ce responsable, il importe qu'elle soit informée de son nom et de son adresse dès le moment de la collecte des données.

L'article 13 paragraphe 2 donne aux Etats membres le pouvoir d'apporter des restrictions à l'obligation d'informer la personne concernée lors de la collecte de données pour des considérations supérieures liées à l'intérêt

général. En vertu de cette disposition, il n'est pas obligatoire de communiquer à la personne concernée les informations indiquées à l'article 13 paragraphe 1 si cette communication empêche l'exercice des fonctions des autorités publiques chargées de tâches de contrôle et de vérification, ou du maintien de l'ordre public.

Article 14

Droits complémentaires de la personne concernée

L'article 14 porte sur les droits de la personne concernée vis-à-vis du responsable du fichier. La protection des données ayant pour objet de sauvegarder le droit à l'intimité de la vie privée, les droits de la partie concernée à l'égard du responsable du fichier constituent un élément fondamental de la protection des données.

Aux termes de l'article 14 paragraphe 1, la personne concernée a le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement. Les raisons légitimes visées dans cette disposition sont l'absence d'une justification légale d'un certain traitement des données à caractère personnel, par exemple parce que les conditions prévues aux chapitres II et III du projet de directive concernant la légitimité de ce traitement ne sont pas remplies pour un traitement de données déterminé.

L'article 14 paragraphe 2 donne le droit à la personne concernée de ne pas être soumise à des décisions la concernant prises par les institutions publiques ou privées qui impliquent une appréciation de son comportement qui ait pour seul fondement un traitement automatisé de données à caractère personnel qui donne une définition du profil ou de la personnalité de l'intéressé. Cette décision vise à protéger le droit de la personne concernée à participer au processus de prise de décisions qui ont de l'importance pour elle. L'utilisation de profils de données détaillées sur les particuliers par de puissantes institutions publiques et privées enlève aux particuliers la capacité d'influencer les processus décisionnels dans ces institutions, si les décisions sont prises sur le seul fondement de leur profil de données.

Pour que la personne concernée puisse faire valoir efficacement ses droits à rectification, effacement ou verrouillage de données vis-à-vis du responsable du fichier, il est essentiel qu'elle ait accès aux données contenues dans le fichier, droit qui lui est reconnu par l'article 14 paragraphes 3 et 4. L'article 14 paragraphe 3 accorde à la personne concernée le droit d'être informée des faits pertinents concernant le traitement de ses données personnelles par le responsable du fichier, de façon à pouvoir faire valoir son droit de rectification, d'effacement et de verrouillage et exercer un contrôle effectif sur le traitement des données à caractère personnel la concernant. L'article 14 paragraphe 4 donne à la personne concernée le droit d'obtenir, à des intervalles raisonnables, sans délais ou frais excessifs, la confirmation de l'existence ou non dans le fichier de données la concernant et, si de telles données figurent dans le dossier, la communication de ces données sous une forme intelligible.

Les dispositions de l'article 14 paragraphes 3 et 4 laissent aux Etats membres le soin de décider de la façon dont ces informations sont transmises à la personne concernée.

En outre, la définiton de l'expression "intervalles raisonnables" est laissée au droit national des Etats membres. Compte tenu des intérêts de la personne concernée et du responsable du dossier, le droit national des Etats membres peut prévoir que le responsable du dossier ne réclame à la personne concernée qui fait valoir son droit d'accès que le paiement des coûts qui en résultent et qui ne doivent pas être excessifs.

L'article 14 paragraphe 4 autorise les Etats membres à prévoir une règle particulière pour l'exercice du droit d'accès de la personne concernée dans le cas des données à caractère médical. Pour protéger la personne concernée contre des chocs psychologiques; qui peuvent entraîner dans des cas extrêmes des actes suicidaires, ces informations peuvent lui être communiquées par un médecin.

L'article 14 paragraphe 5 du projet de directive accorde à la personne concernée le droit de rectification, effacement ou de verrouillage des données si le traitement de ces données est incompatible avec les dispositions du projet de directive.

Les personnes concernées peuvent demander la rectification si les données les concernant sont incorrectes, incomplètes, inexactes, trompeuses ou dépassées. Le droit de la personne concernée d'obtenir l'effacement ou le verrouillage des données présuppose que ces données aient été traitées en violation des dispositions du projet de directive. A cet égard, l'article 14 paragraphe 5 vise toutes les dispositions du projet de directive qui réglementent la collecte, l'enregistrement, le traitement et l'utilisation de données à caractère personnel.

La notion de verrouillage tire son origine de la loi fédérale allemande concernant la protection des données (articles 14, 27 et 35: Sperrung). Si les données sont verrouillées parce qu'elles ont été collectées, enregistrées, traitées ou utilisées en violation des dispositions du projet de directive, le responsable du fichier peut les y conserver, mais il lui est interdit de les traiter ou de les utiliser et en particulier de les communiquer à des tiers. Les données verrouillées doivent être signalées comme telles dans le fichier, pour que l'utilisateur de celui-ci soit informé du verrouillage.

La rédaction du projet de directive ("le cas échéant") laisse au législations des Etats membres relatives à la protection des données le soin de définir précisément les droits de la personne concernée d'obtenir l'effacement, le verrouillage ou la rectification en fonction des différentes situations dans lesquelles des données à caractère personnel sont traitées et utilisées en violation des dispositions du projet de directive.

Il arrive fréquemment que des données soient non seulement traitées par le responsable du fichier mais également communiquées à des tiers. Si le responsable du fichier doit corriger, effacer ou verrouiller des données parce qu'elles sont incorrectes ou traitées ou utilisées de façon illégitime, il est dans l'intérêt de la personne concernée que les tiers auxquel ces données ont été transmises soient avisés de la rectification, de l'effacement ou du blocage, de façon à ce qu'ils puissent également rectifier, effacer ou verrouiller les données. Cet intérêt de la personne concernée trouve son expression dans l'article 14 paragraphe 7.

L'article 14 paragraphe 6 accorde à la personne concernée le droit d'obtenir l'effacement des données la concernant enregistrées dans des fichiers constitués à des fins de prospection commerciale ou de publicité directe. La personne concernée peut donc se protéger contre des correspondances publicitaires non sollicitées.

Enfin, en vertu de l'article 14 paragraphe 8, les Etats membres sont tenus de prévoir pour la personne concernée un recours juridictionnel efficace au cas où le responsable du fichier ou une autre personne passe outre aux droits de la personne concernée qui sont énoncés à l'article 14 du projet de directive.

Article 15

Exceptions au droit d'accès de la personne concernée aux fichiers du secteur public

L'article 15 autorise les Etats membres à limiter le droit de la personne concernée à avoir accès au fichier, lorsqu'il s'agit de sauvegarder l'intérêt général supérieur ou des intérêts de particuliers équivalant au droit à la vie privée de la personne concernée, dans la mesure où les données sont conservées dans des fichiers du secteur public. Le projet laisse aux Etats membres le soin de décider de la mesure dans laquelle ils incorporent dans la législation nationale concernant la protection des données des exceptions reposant sur l'article 15. Cependant, les exceptions prévues dans cette disposition se limitent à celles qui sont nécessaires à la protection de valeurs importantes dans une société démocratique et doivent être prévues par une loi. L'énumération des intérêts qui justifient une limitation du droit d'accès en vertu de l'article 15 du projet de directive a un caractère exhaustif.

L'expression "sûreté de l'Etat" vise la protection de la souveraineté nationale contre les menaces internes et externes.

Les mots "poursuites pénales" se rapportent aux poursuites relatives aux crimes et délits qui ont déjà été commis, tandis que la notion de "sécurité publique" englobe toutes les fonctions de police des organes de l'Etat, y compris la prévention de la criminalité. L'expression "intérêt économique et financier sérieux d'un Etat membre ou de la Communauté" désigne tous les moyens de politique économique et de financement des politiques d'un Etat membre ou de la Communauté, par exemple les contrôles de change, les contrôles relatifs au commerce extérieur ou la perception des impôts. Toutefois, seul un intérêt sérieux de ce type justifie la limitation du droit d'accès.

Enfin, l'intérêt d'un tiers équivalant au droit d'accès de la personne concernée et les droits et libertés d'autrui sont considérés comme des justifications de la limitation du droit d'accès. Il s'agit ici d'intérêts tels que des secrets commerciaux d'autres parties ou de la liberté de la presse.

Si la personne concernée se voit refuser l'accès aux données la concernant conservées dans un fichier parce qu'un intérêt visé à l'article 15 paragraphe 1 est en cause, l'autorité responsable de la protection des données est tenue, à la demande de l'intéressé, de procéder à l'inspection et au contrôle nécessaires en ce qui concerne le fichier dans lequel les données en cause sont conservées.

L'article 15 paragraphe 3 autorise les Etats membres à limiter le droit d'accès pour les données compilées temporairement afin d'y extraire des informations statistiques, dans la mesure où ces activités ne représentent qu'un risque mineur pour la personne concernée.

CHAPITRE V

Qualité des données

Les principes de protection des données énoncés dans ce chapitre vont plus loin que ce qu'indique son titre: ils ont trait non seulement à la qualité des données (article 16) mais également au traitement de certaines catégories de données, qui sont jugées particulièrement sensibles pour la personne concernée (article 17), et aux mesures appropriées en matière de sécurité des données (article 18).

Article 16

Principes

En vertu de l'article 16 du projet de directive, les Etats membres sont tenus de faire figurer les principes de base relatifs à la qualité des données à caractère personnel dans leur législation concernant la protection des données. Ces principes doivent assurer le respect du droit à la vie privée de la personne concernée, en imposant certaines restrictions à la collecte et au traitement de données à caractère personnel, ainsi qu'au contenu des fichiers de données à caractère personnel.

L'article 16 paragraphe 1 alinéa a) prévoit que la collecte et le traitement de données à caractère personnel doivent être effectués loyalement et licitement.

Cette disposition vise le traitement de données à caractère personnel, telle que cette notion est définie à l'article 2 alinéa d), ainsi que sa collecte.

La règle énoncée à l'article 16 paragraphe 1 alinéa a) exclut notamment l'utilisation d'appareils cachés permettant d'obtenir des données subrepticement et à l'insu de la personne concernée, notamment par des écoutes téléphoniques et autres, etc. Cette disposition interdit également aux responsables de fichiers de mettre en place et d'utiliser des fichiers clandestins contenant des données à caractère personnel.

L'article 16 paragraphe 1 alinéa b) énonce le principe de la détermination de la finalité de l'enregistrement des données. Selon ce principe, des données à caractère personnel ne peuvent être conservées que pour des finalités déterminées, explicites et légitimes.

L'objet de l'enregistrement de données à caractère personnel doit être déterminé, c'est-à-dire que le but de l'enregistrement et de l'utilisation des données doit être défini et spécifié de façon aussi précise que possible. Une définition ou description générale ou vague de l'objet d'un fichier ("à des fins commerciales", par exemple) n'est pas conforme au principe de la définition de la finalité énoncée à l'article 16 paragraphe 1 alinéa b).

Il y a lieu de spécifier la finalité avant l'enregistrement des données. Dans le cas où les données sont collectées auprès de la personne concernée, l'article 13 prévoit que la finalité doit déjà être déterminée au moment où la collecte des données a lieu.

Une modification ultérieure de la finalité d'un traitement n'est légitime que dans la mesure où elle n'est pas incompatible avec la finalité initiale.

L'article 16 paragraphe 1 alinéa b) oblige également le responsable du fichier à indiquer la finalité de la conservation et de l'enregistrement des données. Cette obligation de divulgation vise à empêcher l'enregistrement et l'utilisation de données à caractère personnel dans des buts cachés.

Dans la mesure où la finalité de la conservation et de l'utilisation de données à caractère personnel doit être légitime, les finalités potentielles d'un fichier sont limitées. Un tel fichier ne peut être créé et utilisé que dans des buts compatibles avec les dispositions du projet de directive et des législations nationales des Etats membres. En outre, sont seules légitimes les finalités qui correspondent aux fonctions administratives des responsables du fichier dans le secteur public et au

domaine d'activités commerciales des responsables de fichiers dans le secteur privé. L'article 16 paragraphe 1 alinéa b) indique clairement que le principe de la détermination de la finalité ne s'applique pas uniquement au traitement des données à caractère personnel: il faut en outre que ces données soient compatibles avec la finalité du fichier.

L'article 16 paragraphe 1 alinéa c) stipule que les données figurant dans un fichier doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées. Ce principe vise à faire en sorte que le contenu d'un fichier soit conforme à sa finalité.

Les dispositions de l'article 16 paragraphe 1 alinéa d) sont étroitement liées à celles de l'article 16 paragraphe 1 alinéas b) et c). Les données enregistrées dans un dossier doivent être exactes et, si nécessaire, mises à jour. Au cas où des données sont inexactes ou incomplètes eu égard à la finalité du fichier, l'article 16 paragraphe 1 alinéa d) prévoit qu'elles doivent être effacées ou rectifiées.

L'article 16 paragraphe 1 alinéa e) a trait à la durée maximale de conservation de données à caractère personnel. Selon cette disposition, la conservation de données sous une forme permettant l'identification des personnes concernées n'est autorisée que pendant la période qui semble nécessaire pour atteindre le but dans lequel les données ont été enregistrées.

Dans certains cas, cependant, il est nécessaire, à des fins statistiques par exemple, que les données soient conservées plus longtemps. Dans cette hypothèse, il est essentiel pour la protection de la personne concernée d'éliminer tout lien entre son nom et les autres données.

L'article 16 paragraphe 2 fait obligation au responsable du fichier d'assurer le respect des dispositions relatives à la qualité des données énoncées à l'article 16 paragraphe 1.

Article 17

Catégories particulières de données

Il est communément admis que le droit à la vie privée n'est pas mis en péril par les données à caractère personnel elles-mêmes, mais que des dangers peuvent résulter du contexte dans lequel le traitement de données à caractère personnel a lieu. Cependant, les Etats membres sont d'accord pour estimer que certaines catégories de données présentent - en raison de leur nature même, indépendamment du contexte dans lequel elles sont traitées - des risques d'atteinte à la vie privée. C'est pourquoi l'article 17 du projet de directive limite strictement le traitement électronique et l'utilisation d'informations sensibles dans les fichiers contenant des données à caractère personnel.

L'article 17 énumère les catégories de données sensibles suivantes: origine raciale (y compris information sur la couleur de la peau); opinion politique; convictions religieuses ou philosophiques (y compris l'absence de convictions religieuses); (ces catégories comprennent les informations sur les activités de la personne concernée liées aux convictions politiques, religieuses ou philosophiques); information sur les appartenances syndicales, la santé de la personne concernée (y compris des informations sur l'état de santé physique et mentale passé, présent et futur et des informations en matière de toxicomanie ou d'alcoolisme); information concernant la vie sexuelle.

D'une manière générale, l'article 17 paragraphe 1 interdit le traitement informatisé de données sensibles. Les exceptions à cette règle sont les cas où l'intéressé a donné son accord, qui doit être libre, exprès et écrit, et l'exception énoncée à l'article 17 paragraphe 2.

Selon cette dernière disposition, les Etats membres peuvent autoriser le traitement électronique de données sensibles pour des motifs d'intérêt public important. Néamoins, cette exception implique l'adoption d'une loi précisant les types de données sensibles pouvant être traitées électroniquement, les personnes ayant accès aux données et les garanties appropriées contre les utilisations abusives et les accès autorisés.

L'article 17 paragraphe 3 énonce une règle particulière pour la conservation d'informations sur les condamnations pénales. La conservation de telles informations dans des fichiers informatisés n'est permise que dans des fichiers relevant du secteur public.

Le champ d'application de l'article 17 est limité: il ne s'étend qu'aux données qui sont traitées de façon informatisée.

D'autre part, l'article 17 n'est pas applicable à l'enregistrement et au traitement électroniques de données concernant les opinions politiques, les convictions religieuses et philosophiques et l'appartenance syndicale, dans la mesure où ces données sont traitées par des associations sans but lucratif dans le respect des conditions énoncées à l'article 3 paragraphe 2 alinéa b).

Article 18

Sécurité des données

La vie privée de la personne concernée est uniquement menacée par le responsable du fichier, qui rassemble enregistre, traite et communique les données relatives à l'intéressé dans les buts qui lui sont propres.

Son droit à la vie privée est également mis en péril si les données la concernant sont utilisées abusivement par des tiers qui, sans autorisation, accèdent aux données et les utilisent.

En vertu de la première phrase de l'article 18 paragraphe 1, les Etats membres doivent obliger le responsable du fichier à prendre les mesures techniques et d'organisation appropriées nécessaires à la protection des données contenues dans le fichier contre les menaces représentées par l'intrusion de tiers dans le fichier ou la perte accidentelle de données: destruction accidentelle ou non autorisée, perte accidentelle, altération, accès et tout autre traitement non autorisé de données.

Les mesures techniques de sécurité des données comprennent les mesures de sécurité relatives à l'accès aux locaux de traitement et de conservation des données, des codes d'identification pour les personnes autorisées à se rendre dans ces locaux, des garanties telles que l'utilisation de mots de passe pour l'accès à des fichiers informatisés, le cryptage de données, et la surveillance du piratage et d'autres activités inhabituelles. En ce qui concerne les mesures d'organisation, le responsable du fichier doit adopter certaines procédures au sein de la hiérarchie de son administration ou de son entreprise, par exemple en établissant des niveaux d'autorité pour l'accès aux données.

La deuxième phrase de l'article 18 paragraphe 1 prévoit un niveau approprié de sécurité des données pour les fichiers informatisés. Pour ces fichiers, les mesures à prendre doivent assurer un niveau de sécurité approprié compte tenu, d'une part, de l'état de la technique dans le domaine de la sécurité des données et du coût de la mise en oeuvre de ces mesures et, d'autre part, de la nature des données conservées dans le fichier et de l'évaluation des risques potentiels. Pour déterminer le niveau approprié des mesures de sécurité des données, le responsable du fichier doit prendre en considération les recommandations en matière de sécurité informatique et d'interopérabilité des réseaux qui pourront être adoptés par la Communauté selon les modalités prévues à l'article 29 du projet de directive.

L'obligation de prendre des mesures de sécurité appropriées ne se limite pas à la localisation du traitement des données ou au matériel et au logiciel utilisés pour le traitement. Si des transmissions de données ont lieu entre ordinateurs ou entre un ordinateur et des terminaux via un réseau de télécommunications, en vertu de l'article 18 paragraphe 2 des mesures de sécurité doivent également être prises en ce qui concerne le réseau afin d'assurer un transfert de données sûr et ininterrompu.

L'article 18 paragraphe 3 concerne l'accès direct d'un utilisateur extérieur à un fichier lors d'une consultation en ligne. L'autorisation en vertu de laquelle l'utilisateur peut obtenir des données du fichier doit être spécifiée et limitée par le contrat passé avec le responsable du fichier. Le projet de directive fait obligation au responsable du fichier

de concevoir le matériel et le logiciel utilisés pour la consultation en ligne de telle façon que l'accès de l'utilisateur reste dans les limites fixées par l'autorisation que le responsable du fichier lui a accordée.

L'article 18 paragraphe 4 désigne les personnes à qui il incombe de veiller au respect des obligations établies par l'article 18 paragraphes 1 à 3. Les personnes qui, de fait ou par contrat, ont le contrôle sur les opérations relatives à un fichier sont également responsables du respect des règles relatives à la sécurité des données. Les personnes visées par cette règle sont selon le cas, le responsable du fichier, l'utilisateur pouvant consulter des données en ligne et les entreprises effectuant des traitements de données pour le compte du responsable du fichier.

Enfin, l'article 18 paragraphe 5 établit une obligation de secret professionnel pour les salariés du responsable du fichier et les autres personnes qui, dans le cadre de leurs activités professionnelles, ont accès aux informations à caractère personnel contenues dans un fichier. Il est interdit à ces personnes de communiquer à des tiers les informations auxquelles elles ont accès, sans l'accord du responsable du fichier.

CHAPITRE VI

Dispositions spécifiques pour certains secteurs

Article 19

Les Etats membres peuvent prévoir des dérogations aux dispositions de la présente directive pour les organismes de presse et de l'audiovisuel dans la mesure où elles sont nécessaires pour concilier les droits fondamentaux des personnes, notamment le droit à la vie privée, avec la liberté d'information et la liberté de la presse. Il existe, en effet, des risques de conflit entre les deux catégories de droits fondamentaux. La solution adoptée met l'accent sur l'obligation de faire une balance des intérêts en

présence en cas de dérogation. Cette balance pourra prendre en compte notamment l'existence des recours possibles pour la personne concernée ou d'un éventuel droit de réponse, l'existence de code de déontologie professionnelle, les limites fixées par la Convention européenne des droits de l'homme, les principes généraux du droit .

Article 20

Cet article prévoit que les Etats membres encouragent les milieux professionnels à élaborer des codes de déontologie ou de bonnes conduites européens qui pourraient faciliter l'application des principes de la directive dans certains secteurs.
La Commission soutiendra également de telles initiatives et en tiendra compte, le cas échéant, dans l'exercice de son pouvoir réglementaire ou pour faire de nouvelles propositions.

CHAPITRE VII

Responsabilité et sanction

Article 21
Responsabilité

En cas de préjudice dû au non respect des dispositions de la présente directive, cet article fait peser la responsabilité sur le responsable du fichier à qui la personne concernée peut demander des dommages et intérêts. La notion de préjudice couvre aussi bien le préjudice matériel que moral. Une limite à la responsabilité du responsable du fichier est prévue en cas de perte, destruction, ou accès non autorisé, à condition qu'il apporte la preuve que les mesures de sécurité ont été respectées.

Article 22

Traitement pour le compte du responsable du fichier

L'objet de cet article est d'éviter qu'un traitement par un tiers pour le compte du responsable du fichier ait pour conséquence d'affaiblir la protection de la personne concernée. A cette fin, des obligations pèsent à la fois sur le responsable du fichier et sur le tiers effectuant le traitement.

Article 23
Sanctions

Afin d'assurer le respect des dispositions prises en application de la présente directive, les Etats membres ont l'obligation de prévoir des sanctions réellement dissuasives, pénales par exemple, en tenant compte en particulier du fait que le non-respect des principes de la protection de la personne concernée constitue une atteinte à un droit fondamental.

CHAPITRE VIII

Transfert de données à caractère personnel vers des pays tiers

Article 24

Principes

Cet article pose le principe selon lequel le transfert de données à caractère personnel depuis un Etat membre vers un pays tiers ne peut avoir lieu que si ce pays assure un niveau de protection adéquat. Il incombe aux Etats membres, et le cas échéant à la Commission, de déterminer si un pays assure un niveau de protection adéquat. Les Etats membres doivent informer la Commission des cas où un pays tiers importateur n'assure pas ce niveau de protection. Dans ce cas un processus de négociation peut s'engager entre la Commission et le pays tiers concerné.

La Commission peut décider dans le cadre des pouvoirs d'exécution qui lui sont conférés, à l'article 29, qu'un pays assure un niveau de protection adéquat en se fondant sur sa législation nationale et/ou sur les engagements internationaux auxquels est partie ce pays. La convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement des données à caractère personnel fait partie des engagements que la Commission prendra en compte. Elle pourra également avoir recours à l'expertise du Groupe de protection des données à caractère personnel dans ce domaine.

Article 25

Dérogation

Si un pays n'assure pas un niveau de protection adéquat, une dérogation permettant le transfert de données est possible pour une exportation spécifique. L'Etat membre de localisation du fichier peut autoriser un tel transfert si le responsable du fichier peut garantir un niveau de protection adéquat pour cette exportation et si les autres Etats membres ou la Commission ne s'y opposent pas. Pour cela une procédure d'information est prévue avec un délai de notification d'opposition de 10 jours.
En cas de notification d'opposition la Commission peut prendre les mesures appropriées, notamment décider d'interdire le transfert.

CHAPITRE IX

Autorité de contrôle et Groupe de protection des données à caractère personnel

Article 26

L'autorité de contrôle

Cet article prévoit l'institution d'une autorité de contrôle qui se caractérise par son indépendance ainsi que par des moyens d'investigation et d'intervention adaptés à la mission de surveillance qui lui est confiée. Les législations nationales doivent garantir ces deux caractéristiques. L'expression "autorité de contrôle" ne préjuge pas de l'adoption d'une structure interne multiple en fonction du système constitutionnel des Etats membres.

Article 27

Groupe de protection des données à caractère personnel

En raison des particularités du domaine de la protection des personnes à l'égard des données à caractère personnel, cet article établit un comité de type consultatif, le Groupe de protection des données à caractère personnel. Ce Groupe de protection des données à caractère personnel se caractérise par son indépendance et est composé des représentants des autorités de contrôle nationales. Un représentant de la Commission préside ce Groupe.

Article 28

Missions du Groupe de protection des données à caractère personnel

Cet article fixe les tâches du Groupe de protection des données à caractère personnel. Le Groupe apporte à la Commission ses connaissances et son expertise dans le domaine de la protection des personnes à l'égard du traitement des données à caractère personnel. Il contribue ainsi à l'application homogène des règles nationales prises en application de la présente directive; il apprécie le niveau de protection dans la Communauté et dans les pays tiers et en informe la Commission; il peut enfin conseiller la Commission sur des projets de mesures additionnelles à prendre.

Le Groupe de protection des données à caractère personnel peut émettre des recommandations qui peuvent, s'il le souhaite, être transmises au comité consulatatif qui intervient dans le cadre des pouvoirs d'exécution conférés à la Commission.

Un rapport annuel sur l'état de la protection des données à caractère personnel dans la Communauté et dans les pays tiers est établit par le Groupe de protection des données à caractère personnel. Ce rapport est transmis à la Commission.

CHAPITRE X

Pouvoir réglementaire de la Commission

Articles 29 et 30

Exercice du pouvoir réglemententaire
Comité consultatif

L'article 29 confère à la Commission les compétences d'exécution relatives aux modalités techniques d'application qui sont nécessaires en raison de l'étendue et du caractère technique du domaine du traitement des données à caractère personnel.

La directive ayant pour objet de contribuer à la réalisation du marché intérieur, l'article 30 prévoit l'intervention d'un comité de type consultatif pour assister la Commission dans l'exercice de ses compétences d'exécution et applique les procédures fixées dans la décision du Conseil du 13 juillet 1987 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission.

Proposta de SYN 287

DIRECTIVA DO CONSELHO

relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais.

O CONSELHO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Económica Europeia e, nomeadamente, o seu artigo 100º-A e o seu artigo 113º,

Tendo em conta a proposta da Comissão (1),

Em colaboração com o Parlamento Europeu (2),

Tendo em conta o parecer do Comité Económico e Social (3),

(1) Considerando que os objectivos da Comunidade, enunciados no Tratado com a redacção que lhe foi dada pelo Acto Único Europeu, consistem em estabelecer uma união cada vez mais estreita entre os povos europeus, em estabelecer relações mais estreitas entre os Estados que a Comunidade agrupa, em assegurar, mediante uma acção comum, o progresso económico e social eliminando as barreiras que dividem a Europa, em promover a melhoria constante das condições de vida destes povos, em consolidar a defesa da paz e da liberdade e em promover a democracia com base nos direitos fundamentais reconhecidos nas Constituições e leis dos Estados-membros, bem como na Convenção Europeia de Defesa dos Direitos do Homem e das Liberdades Fundamentais;

(2) Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 8º-A do Tratado, a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais é assegurada, necessitam que não apenas os dados pessoais possam circular, quaisquer que sejam os Estados-membros em que sejam tratados ou solicitados mas, igualmente, que os direitos fundamentais sejam salvaguardados, tendo em conta o recurso cada vez mais frequente na Comunidade aos tratamentos de dados pessoais nos diversos domínios das actividades económicas e sociais;

(3) Considerando que o mercado interno engloba um espaço sem fronteiras; que, por este facto, as administrações nacionais dos diferentes Estados-membros, por força do direito comunitário, são chamadas cada vez mais frequentemente a colaborarem e a trocarem entre si dados pessoais a fim de poderem desempenhar a sua missão ou exercer tarefas por conta de uma administração de outro Estado-membro;

(4) Considerando que o reforço da cooperação científica e técnica, bem como a criação coordenada de novas redes de telecomunicações na Comunidade necessitam e facilitam a circulação transfronteiriça de dados pessoais;

(5) Considerando que a diferença de níveis de protecção da vida privada relativamente aos tratamentos de dados pessoais assegurados nos Estados-membros pode impedir a transmissão destes dados do território de um Estado-membro para o de outro Estado-membro; que esta diferença pode, por conseguinte, constituir um obstáculo ao exercício de uma série de actividades económicas à escala comunitária, falsear a concorrência e entravar a função das administrações intervenientes no âmbito de aplicação do direito comunitário; que esta diferença de níveis de protecção resulta da disparidade das disposições nacionais legislativas, regulamentares e administrativas;

(6) Considerando que para eliminar os obstáculos à circulação dos dados pessoais o nível de protecção da vida privada relativamente aos tratamentos destes dados deve ser equivalente em todos os Estados-membros; que é, assim, necessário aproximar as legislações aplicáveis na matéria;

(7) Considerando que o objecto das legislações nacionais relativas ao tratamento dos dados pessoais é assegurar o respeito dos direitos fundamentais, nomeadamente, o direito à vida privada reconhecido não só no artigo 8º da Convenção de Defesa dos Direitos do Homem e das Liberdades Fundamentais como também nos princípios gerais do direito comunitário; que, por conseguinte, a aproximação destas legislações não deve conduzir à redução da protecção que estas asseguram mas deve, em contrapartida, ter por objectivo a garantia de um alto nível de protecção na Comunidade;

(8) Considerando que os princípios da protecção da vida privada relativamente ao tratamento dos dados pessoais objecto da directiva poderão ser completados ou precisados, nomeadamente relativamente a certos sectores, através de regras específicas conformes a esses princípios;

(9) Considerando que os princípios da protecção devem aplicar-se a todos os ficheiros, desde que as actividades do responsável pelo ficheiro relevem do âmbito de aplicação do direito comunitário; que os ficheiros do sector público que não relevem do âmbito de aplicação do direito comunitário deveriam estar sujeitos aos mesmos princípios da protecção utilizados nas legislações nacionais, tal como se encontra previsto na Resolução dos Representantes dos Governos dos Estados-membros das Comunidades Europeias reunidos em Conselho de ....; que, todavia, devem ser excluídos os ficheiros que relevem exclusivamente do exercício do direito à vida privada de uma pessoa singular, tal como os ficheiros pessoais de endereços;

(10) Considerando que é necessário que qualquer tratamento de dados pessoais na Comunidade respeite a legislação do Estado-membro em que o ficheiro se encontra localizado, a fim de evitar que uma pessoa escape à protecção que lhe deve ser garantida por força da presente directiva; que, relativamente a este ponto, cada parte de um ficheiro repartido por vários Estados-membros deve ser considerada como um ficheiro e que a transferência da sua localização para um país terceiro não deve prejudicar esta protecção;

(11) Considerando que qualquer tratamento de dados pessoais deve ser lícito; que tal licitude deve fundar-se no consentimento da pessoa em causa ou no direito comunitário ou nas legislações nacionais;

(12) Considerando que as legislações nacionais podem especificar, nos termos da directiva, as regras relativas à licitude do tratamento; que, contudo, essa possibilidade não pode servir de fundamento para um controlo de um Estado-membro que não o Estado-membro de localização do ficheiro, dado que a obrigação deste último de assegurar, em conformidade com a presente directiva, a protecção da vida privada relativamente ao tratamento dos dados pessoais, é suficiente, à luz do direito comunitário, para permitir a livre circulação dos dados;

(13) Considerando que os processos de notificação, para os ficheiros do sector público ou privado, e de informação aquando da primeira comunicação, para os ficheiros do sector privado, têm por objectivo assegurar a transparência indispensável ao exercício do direito de acesso da pessoa em causa aos dados que a ela dizem respeito;

(14) Considerando que a pessoa em causa deve beneficiar de uma informação eficaz e completa para que o seu consentimento seja válido, bem como nos casos em que fornece dados a seu respeito;

(15) Considerando que a pessoa em causa deve poder beneficiar do direito de acesso a fim de poder assegurar-se da licitude do tratamento dos dados que lhe dizem respeito e da sua qualidade;

(16) Considerando que para ser objecto de um tratamento, os dados devem responder a certas exigências; que o tratamento dos dados que são susceptíveis, pela sua própria natureza, de prejudicar o direito à vida privada deve ser proibido salvo consentimento explícito da pessoa em causa; que, contudo, por razões de interesse público importante, nomeadamente nas profissões médicas, podem ser previstas derrogações com base em lei que fixe precisa e estritamente as condições e limites do tratamento deste tipo de dados;

(17) Considerando que a protecção da vida privada relativamente a dados pessoais exige que sejam tomadas medidas de segurança apropriadas, quer a nível da concepção quer da tecnologia do tratamento, a fim de impedir qualquer tratamento não permitido;

(18) Considerando que no domínio dos meios de comunicação social os Estados-membros podem prever derrogações às disposições da presente directiva, na medida em que tenham por objectivo conciliar o direito à vida privada com a liberdade da informação e o direito de receber ou de comunicar informações, tal como é garantido nomeadamente no artigo 10º da Convenção de Defesa dos Direitos do Homem e das Liberdades Fundamentais;

(19) Considerando que os Estados-membros devem incentivar a elaboração, por parte dos meios profissionais, de códigos europeus de deontologia ou de boa conduta relativos a determinados sectores específicos; que a Comissão apoiará essas iniciativas, tomando-as em consideração quando examinar a possibilidade de novas medidas específicas para determinados sectores;

(20) Considerando que, em caso de não respeito das disposições previstas na presente directiva, o responsável pelo ficheiro deve ser considerado, como civilmente responsável; que devem ser aplicadas sanções dissuasivas a fim de assegurar uma protecção efectiva;

(21) Considerando que é igualmente necessário que a transferência de dados pessoais se possa efectuar com países terceiros que possuam um nível de protecção adequado; que, na ausência de uma protecção desse tipo em países terceiros, a presente directiva prevê, em especial, processos de negociação a realizar com eles;

(22) Considerando que os princípios constantes da presente directiva concretizam e ampliam os constantes da Convenção de 28 de Janeiro de 1981 do Conselho da Europa relativa à protecção das pessoas no que diz respeito ao tratamento automatizado dos dados pessoais;

(23) Considerando que a existência em cada Estado-membro de uma autoridade de controlo independente constitui um elemento essencial da protecção das pessoas no que diz respeito ao tratamento de dados pessoais; que, a nível comunitário, deve ser criado um Grupo de protecção dos dados pessoais, composto por representantes das autoridades de controlo nacionais, que exercerá as suas funções de forma independente; que, tendo em conta este carácter específico, deve aconselhar a Comissão e contribuir para a aplicação homogénea das regras nacionais de execução da presente directiva;

(24) Considerando que a adopção das medidas complementares para a aplicação dos princípios da presente directiva necessita da atribuição de um poder regulamentar à Comissão e da criação de um Comité Consultivo de acordo com as modalidades fixadas na Decisão 87/373/CEE do Conselho [1],

---

(1) JO nº L 197 de 18.7.1987, p. 33.

ADOPTOU A PRESENTE DIRECTIVA

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1o

Objecto da directiva

1. Os Estados-membros assegurarão, em conformidade com as disposições da presente directiva, a protecção da vida privada das pessoas no que diz respeito ao tratamento dos dados pessoais contidos em ficheiros.

2. Os Estados-membros não podem restringir ou proibir a livre circulação dos dados pessoais entre Estados-membros por razões relativas à protecção assegurada por força do número anterior.

Artigo 2o

Definições

Para efeitos da presente directiva, entende-se por:

a) "dados pessoais" qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é, nomeadamente, considerada identificável uma pessoa que pode ser identificada por referência a um número de identificação ou a uma informação similar;

b) "tornar anónimo" uma alteração dos dados pessoais de forma a que as informações que neles estão contidas possam deixar de estar associadas a uma pessoa singular determinada ou determinável, ou apenas mediante um esforço excessivo em pessoal, em custos e em tempo;

c) "ficheiro de dados pessoais" (ficheiro) qualquer conjunto de dados pessoais, centralizados ou repartidos por vários locais, objecto de um tratamento automatizado ou que, ainda que não o sejam, se encontrem estruturados e acessíveis num conjunto organizado segundo critérios determinados de forma a facilitar a utilização ou a interconexão dos dados;

d) "tratamento" as operações efectuadas ou não com a ajuda de processos automatizados: registo, conservação, interconexão de dados, a sua alteração, a sua utilização e a sua comunicação, nomeadamente a transmissão, a difusão, a extracção, bem como o bloqueio e a limpeza;

e) "responsável pelo ficheiro" a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo competente, segundo o direito comunitário ou a legislação nacional de um Estado-membro, para decidir qual será a finalidade do ficheiro, que categorias de dados pessoais devem ser registadas, que operações lhes serão aplicadas e os terceiros que a ele podem ter acesso;

f) "autoridade de controlo" a autoridade pública independente ou qualquer outra instância independente, designadas por cada Estado-membro em conformidade com o artigo 26º da presente directiva;

g) "sector público" o conjunto das administrações, organizações e entidades de um Estado-membro que relevam do direito público, à excepção das que participam numa actividade industrial ou comercial, bem como os organismos e entidades de direito privado quando participem no exercício da autoridade pública;

h) "sector privado" qualquer pessoa singular ou colectiva, ou associação, incluindo as administrações, organizações e entidades do sector público, na medida em que exerçam uma actividade industrial ou comercial.

Artigo 3o

Âmbito de aplicação

1. Os Estados-membros aplicarão as disposições da presente directiva aos ficheiros do sector privado e do sector público, à excepção dos ficheiros do sector público cujas actividades não relevem do âmbito de aplicação do direito comunitário.

2. As disposições da presente directiva não se aplicam aos ficheiros:

a) na posse de uma pessoa singular exclusivamente para fins privados ou pessoais ou

b) na posse de associações sem fim lucrativo, nomeadamente, de natureza política, filosófica, religiosa, cultural, sindical, desportiva ou de lazer, no âmbito do seu objectivo legítimo e desde que digam unicamente respeito aos membros e correspondentes da associação que tenham consentido nele figurar e desde que não sejam comunicados a terceiros.

Artigo 4º

Direito aplicável

1. Cada Estado-membro aplicará as disposições da presente directiva :

(a) a todos os ficheiros localizados no seu território;

(b) ao responsável pelo ficheiro que resida no seu território e utilize a partir desse território um ficheiro localizado num país terceiro cuja legislação não possua um nível de protecção adequado, a menos que essa utilização seja esporádica.

2. Cada Estado-membro aplicará as disposições previstas nos artigos 5º, 6º, 8º, 9º, 10º, 17º, 18º e 21º da presente directiva ao utilizador que consulte um ficheiro localizado num país terceiro a partir de um terminal localizado num território de um Estado-membro, a menos que esta utilização seja esporádica.

3. Quando um ficheiro for temporariamente transferido de um Estado-membro para outro Estado-membro, este último não colocará qualquer obstáculo e não exigirá qualquer formalidade adicional às regras aplicáveis no Estado-membro de localização permanente do ficheiro.

CAPÍTULO II

LICITUDE DO TRATAMENTO NO SECTOR PÚBLICO

Artigo 5º

Princípios

1. Sem prejuízo das disposições previstas no artigo 6º, os Estados-membros devem prever na sua legislação relativa aos ficheiros que relevam do sector público que:

(a) a criação de um ficheiro e qualquer outro tratamento de dados pessoais são lícitos na medida em que sejam necessários para a execução das tarefas da autoridade pública responsável por este ficheiro;

(b) o tratamento de dados para outra finalidade que não aquela para a qual o ficheiro foi criado é lícita se:
- a pessoa em causa o consintir ou
- for efectuado com base no direito comunitário ou numa lei, ou num acto de execução de uma lei de um Estado-membro conforme à presente directiva que o permita e que fixe os seus limites ou
- um interesse legítimo da pessoa em causa não se opuser a essa alteração de finalidade ou
- for necessária a fim de evitar uma ameaça iminente da ordem pública ou uma ameaça grave ao direito de outrem.

Artigo 6o

Tratamento no sector público que tenha por objectivo a comunicação de dados pessoais

1. Os Estados-membros devem prever que a comunicação de dados pessoais contidos em ficheiros de uma entidade do sector público só é lícita:

   a) se for necessária para o exercício das tarefas da entidade do sector público que comunica ou que solicita a comunicação desses dados ou,

   b) a pedido de uma pessoa singular ou colectiva do sector privado que invoque um interesse legítimo desde que o interesse da pessoa em causa não prevaleça.

2. Sem prejuízo do disposto no nº 1, os Estados-membros podem precisar os termos em que a comunicação de dados pessoais é lícita.

3. Os Estados-membros devem prever na sua legislação que, no caso referido na alínea b) do nº 1, o responsável pelo ficheiro informe as pessoas em causa da comunicação dos dados pessoais. Os Estados-membros podem prever que esta informação seja substituída por uma autorização prévia da autoridade de controlo.

Artigo 7o

Obrigação de notificação à autoridade de controlo

1. Os Estados-membros devem prever que a criação de um ficheiro do sector público, cujos dados pessoais são susceptíveis de serem comunicados, deva ser previamente notificada à autoridade de controlo para efeitos de registo. O registo pode ser consultado por qualquer pessoa.

2. Os Estados-membros definirão as informações que devem ser notificadas à autoridade de controlo. Estas informações devem incluir pelo menos o nome e endereço do responsável pelo ficheiro, a finalidade do ficheiro, uma descrição do tipo de dados que este contém, os terceiros a quem os dados são susceptíveis de serem comunicados, bem como uma descrição das medidas tomadas nos termos do artigo 18º.

3. Os Estados-membros podem prever que o disposto nos nºs 1 e 2 seja aplicável a outros ficheiros do sector público e que a consulta do registo possa ser limitada pelas razões referidas no nº 1 do artigo 15º.

CAPÍTULO III

LICITUDE DO TRATAMENTO NO SECTOR PRIVADO

Artigo 8º
Princípios

1. Os Estados-membros devem prever que sem o consentimento da pessoa em causa, o registo num ficheiro ou qualquer outro tratamento de dados pessoais só são lícitos se estiverem de acordo com as disposições da presente directiva e se:

   a. o tratamento estiver incluído no âmbito de um contrato ou de uma relação de confiança quase-contratual com a pessoa em causa e se for necessário à sua realização, ou

   b. os dados provierem de fontes geralmente acessíveis ao público e o seu tratamento se destinar unicamente à correspondência, ou

   c. o responsável do ficheiro prosseguir um interesse legítimo, desde que o interesse da pessoa em causa não prevaleça.

2. Os Estados-membros devem prever que incumbe ao responsável pelo ficheiro assegurar que qualquer comunicação não seja incompatível com a finalidade do ficheiro e que não prejudique a ordem pública. Em caso de consulta em linha, as mesmas obrigações incumbem ao utilizador.

3. Sem prejuízo do disposto no nº 1, os Estados-membros podem precisar os termos em que o tratamento dos dados pessoais é lícito.

Artigo 9º

Obrigação de informação da pessoa em causa

1. Os Estados-membros, relativamente ao sector privado, devem prever que, aquando da primeira comunicação ou aquando de uma possibilidade de consulta em linha, o responsável informará do facto a pessoa em causa, indicando igualmente a finalidade do ficheiro, os tipos de dados que nele figuram e o seu nome e endereço.

2. A informação prevista no nº 1 não é obrigatória no caso previsto no nº 1, alínea b), do artigo 8º. A obrigação de informar não existe nos casos em que a comunicação seja imposta por lei.

3. Se a pessoa em causa objectar à comunicação ou a qualquer outro tratamento, o responsável pelo ficheiro deve cessar o tratamento contestado, salvo se uma disposição legal a isso o autorizar.

Artigo 10º

Excepções especiais à obrigação de informar a pessoa em causa

Se a informação da pessoa em causa, a que se refere o nº 1 do artigo 9º, se revelar impossível ou implicar esforços desproporcionados, ou deparar com interesses legítimos predominantes do responsável pelo ficheiro ou com um interesse similar de um terceiro, os Estados-membros podem prever uma derrogação, mediante autorização da autoridade de controlo.

Artigo 11º

Obrigação de notificação à autoridade de controlo

1. Os Estados-membros devem prever que o responsável pelo ficheiro notifique a criação de um ficheiro de dados pessoais, desde que os dados se destinem a ser comunicados e não provenham de fontes geralmente acessíveis ao público. A notificação deve efectuar-se à autoridade de controlo do Estado-membro em que o ficheiro se encontra localizado ou, na ausência de localização num Estado-membro, à autoridade de controlo do Estado-membro em que o responsável residir. O responsável pelo ficheiro deve notificar às autoridades nacionais competentes quaisquer alterações de finalidade do ficheiro ou de endereço.

2. Os Estados-membros definirão as informações que devem ser notificadas à autoridade de controlo. Estas informações devem incluir pelo menos o nome e o endereço do responsável pelo ficheiro, a finalidade do ficheiro, uma descrição dos tipos de dados que este contém, os terceiros a quem os dados são susceptíveis de serem comunicados e uma descrição das medidas tomadas nos termos do artigo 18º.

3. Os Estados-membros podem prever que o disposto nos nºs 1 e 2 se aplique a outros ficheiros do sector privado e que as informações a que se refere o nº 2 sejam acessíveis ao público.

CAPÍTULO IV

DIREITOS DA PESSOA EM CAUSA

Artigo 12º

O consentimento com conhecimento de causa

Qualquer consentimento da pessoa em causa para um tratamento de dados pessoais que a ela digam respeito nos termos da presente directiva só é válido desde que:

(a) a pessoa disponha das seguintes informações:
- as finalidades do ficheiro e os tipos de dados registados,
- o tipo de utilização e, sendo caso disso, os destinatários dos dados pessoais contidos no ficheiro,
- o nome e o endereço do responsável pelo ficheiro;

(b) seja específico e expresso e precise os tipos de dados, as formas de tratamento e os eventuais destinatários que abrange;

(c) possa ser retirado pela pessoa em causa a qualquer momento sem efeitos retroactivos.

Artigo 13o

A informação aquando da recolha

1. Os Estados-membros devem garantir às pessoas junto das quais os dados pessoais são recolhidos o direito de serem informadas pelo menos sobre:

   (a) as finalidades do ficheiro a que as informações se destinam

   (b) o carácter obrigatório ou não da sua resposta às questões que são objecto da recolha

   (c) as consequências que podem sofrer na ausência de resposta

   (d) os destinatários das informações

   (e) a existência do direito de acesso e de rectificação dos dados que lhes dizem respeito e

   (f) o nome e o endereço do responsável pelo ficheiro.

2. O disposto no nº 1 não é aplicável à recolha das informações no caso da informação da pessoa em causa impedir o exercício das funções de controlo e de verificação de uma autoridade pública ou a manutenção da ordem pública.

Artigo 14º

Direitos complementares da pessoa em causa

Os Estados-membros reconhecerão à pessoa em causa os seguintes direitos:

1. de se opôr, por razões legítimas, a que dados pessoais que lhe digam respeito sejam objecto de um tratamento;

2. de não estar sujeita a uma decisão administrativa ou privada que implique uma apreciação do seu comportamento tendo por único fundamento um tratamento automatizado de dados pessoais que dêem uma definição do perfil ou da personalidade do interessado;

3. de conhecer a existência de um ficheiro, as suas finalidades principais, bem como a identidade e a residência habitual, a sede ou a localização do responsável pelo ficheiro;

4. de obter, com uma periodicidade razoável e sem demora ou custos excessivos, a confirmação da existência ou não num ficheiro de dados pessoais que lhe diga respeito, bem como a comunicação desses dados numa forma inteligível.

   Os Estados-membros podem prever que o direito de acesso aos dados de natureza médica só possa ser exercido por intermédio de um médico;

5. de obter, se for caso disso, a rectificação desses dados ou a sua limpeza ou o seu bloqueio quando o seu tratamento não estiver conforme com as disposições da presente directiva;

6. de obter, mediante pedido, a limpeza sem custos dos dados que lhe dizem respeito registados nos ficheiros de prospecção comercial ou publicitária;

7. de obter, em caso de aplicação do nº 5 do presente artigo e se os dados tiverem sido comunicados a terceiros, a notificação destes últimos, da rectificação, da limpeza ou do bloqueio;

8. de dispor de um recurso jurisdicional em caso de violação dos direitos garantidos no presente artigo.

Artigo 15º

Derrogações ao direito de acesso da pessoa em causa aos ficheiros do sector público

1. Os Estados-membros podem limitar, através de uma lei, os direitos previstos nos nºs 3 e 4 do artigo 14º por motivos relativos:

   (a) à segurança do Estado, ou
   (b) à defesa, ou
   (c) a acções penais, ou
   (d) à segurança pública, ou
   (e) a um interesse económico e financeiro imperativo devidamente justificado de um Estado-membro ou da Comunidade Europeia, ou
   (f) à necessidade do exercício das funções de controlo ou de inspecção da autoridade pública, ou
   (g) a um direito equivalente de outra pessoa e dos direitos e liberdades de outrem.

2. Nos casos referidos no nº 1, a autoridade de controlo deve poder proceder, a pedido da pessoa interessada, às verificações necessárias do ficheiro.

3. Os Estados-membros podem limitar o direito de acesso da pessoa interessada aos dados temporariamente coligidos, a fim de deles extrair informações estatísticas.

CAPÍTULO V

QUALIDADE DOS DADOS

Artigo 16º

Princípios

1. Os Estados-membros devem prever que:

a) a recolha e o tratamento de dados pessoais sejam efectuados leal e licitamente;

b) os dados sejam registados para finalidades determinadas, explícitas e legítimas e utilizados de forma compatível com estas finalidades;

c) os dados sejam adequados, pertinentes e não excessivos relativamente às finalidades para as quais são registados;

d) os dados sejam exactos e, se necessário, actualizados; os dados inexactos ou incompletos devem ser limpos ou rectificados;

e) os dados sejam conservados numa forma que permita a identificação das pessoas em causa apenas durante um período que não exceda o necessário para as finalidades relativamente às quais foram registados.

2. Incumbe aos responsáveis pelo ficheiro assegurar o respeito do disposto no nº 1.

Artigo 17o

Categorias específicas de dados

1. Os Estados-membros proibirão o tratamento automatizado, salvo acordo facultativo, expresso e escrito da pessoa em causa, dos dados que revelem a origem racial e étnica, a opção política, as convicções religiosas ou filosóficas, as adesões a nível sindical, bem como as informações relativas à saúde e à vida sexual.

2. Os Estados-membros podem prever, por motivos de interesse público importantes, derrogações ao disposto no nº 1 com base em lei que precise os tipos de dados registáveis, as pessoas que têm acesso ao ficheiro, bem como as garantias apropriadas contra as utilizações abusivas e os acessos não autorizados.

3. Os dados relativos a condenações penais só podem ser conservados em ficheiros do sector público.

Artigo 18o

Segurança dos dados

1. Os Estados-membros devem prever que o responsável pelo ficheiro seja obrigado a tomar as medidas técnicas e organizativas apropriadas, necessárias à protecção do ficheiro contra a destruição, acidental ou não autorizada, a perda acidental, bem como contra a alteração ou o acesso e qualquer outro tratamento não autorizado de dados pessoais.

Estas medidas devem assegurar, relativamente aos ficheiros automatizados, um nível de segurança apropriado, tendo em conta, por um lado, a evolução técnica na matéria e o custo da sua aplicação e, por outro, a natureza dos dados a proteger e a avaliação dos riscos potenciais. Para este efeito, o responsável pelo ficheiro deve tomar em consideração as recomendações em matéria de segurança informática e de interoperabilidade das redes elaboradas pela Comissão segundo as modalidades previstas no artigo 29º.

2. Devem ser escolhidos métodos que garantam uma segurança adequada para a transmissão de dados pessoais numa rede.

3. Em caso de consulta em linha, as instalações técnicas e o suporte lógico devem ser concebidos de forma a que a consulta se realize dentro dos limites da autorização concedida pelo responsável pelo ficheiro.

4. As obrigações a que se referem os nºs 1 a 3 incumbem igualmente às pessoas que, de facto ou por contrato, tenham o controlo das operações relativas a um ficheiro.

5. Qualquer pessoa que no âmbito das suas actividades profissionais tenha acesso a informações contidas em ficheiros não deve comunicá-las a terceiros sem o acordo do responsável pelo ficheiro.

CAPÍTULO VI

DISPOSIÇÕES ESPECÍFICAS RELATIVAMENTE A CERTOS SECTORES

Artigo 19º

Os Estados-membros podem prever para os organismos de imprensa e do sector audiovisual derrogações às disposições da presente directiva, na medida em que sejam necessárias para conciliar o direito à vida privada com as regras que regem a liberdade de informação e de imprensa.

Artigo 20º

Os Estados-membros devem incentivar os meios profissionais a participarem na elaboração de códigos europeus de deontologia ou de boa conduta em relação a certos sectores com base nos princípios contidos na presente directiva.

CAPÍTULO VII

RESPONSABILIDADE E SANÇÕES

Artigo 21º

Responsabilidade

1. Os Estados-membros devem prever que qualquer pessoa, cujos dados pessoais sejam registados num ficheiro e que sofra um prejuízo devido ao tratamento ou a qualquer outra acção incompatíveis com as disposições da presente directiva, tenha direito a uma indemnização a cargo do responsável pelo ficheiro.

2. Os Estados-membros podem prever que os danos resultantes de uma perda ou destruição de dados ou de um acesso não autorizado não sejam imputáveis ao responsável pelo ficheiro, se este provar que tomou as medidas apropriadas para respeitar as exigências enunciadas nos artigos 18º e 22º.

Artigo 22º

Tratamento por conta do responsável pelo ficheiro

1. Os Estados-membros devem prever que o responsável pelo ficheiro deva, em caso de tratamento por sua conta, assegurar-se do respeito das medidas necessárias de segurança e de organização e escolher uma pessoa ou uma empresa que ofereça garantias suficientes a este respeito.

2. Qualquer pessoa que recolha ou trate dados pessoais por conta do responsável pelo ficheiro deve respeitar as obrigações previstas nos artigos 16º e 18º da presente directiva.

3. O contrato deve ser escrito e especificar, em especial, que os dados pessoais só podem ser divulgados pelo prestador ou pelos seus empregados com o acordo do responsável pelo ficheiro.

Artigo 23º

Sanções

Cada Estado-membro deve prever a aplicação de sanções dissuasivas a fim de assegurar o respeito das disposições de execução da presente directiva.

CAPÍTULO VIII

TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

Artigo 24º

Princípios

1. Os Estados-membros devem prever que a transferência para um país terceiro, com carácter temporário ou definitivo, de dados pessoais objecto de um tratamento ou recolhidos com o objectivo de os submeter a um tratamento desse tipo, só pode realizar-se se esse país assegurar um nível de protecção adequado.

2. Os Estados-membros informarão a Comissão dos casos em que um país terceiro importador não assegure um nível de protecção adequado.

3. Quando a Comissão verificar, quer com base em informações dos Estados-membros quer com base noutras informações, que um país terceiro não dispõe de um nível de protecção adequado e que a situação daí resultante se revela prejudicial para os interesses da Comunidade ou de um Estado-membro, pode encetar negociações tendo em vista sanar esta situação.

4. A Comissão pode decidir, de acordo com o processo definido no nº 2 do artigo 30º da presente directiva, que um país terceiro assegura um nível de protecção adequado devido a compromissos internacionais por ele assumidos ou à sua legislação interna.

5. As medidas tomadas nos termos do presente artigo são conformes às obrigações que incumbem à Comunidade por força de acordos internacionais, quer bilaterais quer multilaterais, que regulam a protecção das pessoas relativamente ao tratamento automatizado dos dados pessoais.

Artigo 25º

Derrogação

1. Um Estado-membro pode derrogar ao disposto no nº 1 do artigo 24º, relativamente a uma determinada exportação, mediante apresentação por parte do responsável pelo ficheiro de justificações suficientes que garantam o respeito de um nível de protecção adequado. O Estado-membro só pode conceder uma derrogação após ter informado a Comissão e os Estados-membros desse facto e, na ausência de notificação de oposição expressa por um Estado-membro ou pela Comissão num prazo de dez dias.

2. Em caso de notificação de oposição, a Comissão tomará as medidas apropriadas de acordo com o processo definido no nº 2 do artigo 30º.

CAPÍTULO IX

AUTORIDADES DE CONTROLO E GRUPO DE PROTECÇÃO DOS DADOS PESSOAIS

Artigo 26º

A autoridade de controlo

1. Os Estados-membros assegurarão que uma autoridade independente competente garantirá o controlo da protecção dos dados pessoais. Esta autoridade será encarregada de vigiar a aplicação das disposições nacionais de execução da presente directiva e de preencher todas as atribuições que lhe são conferidas pela presente directiva.

2. A autoridade referida disporá de meios de investigação e de poderes efectivos de intervenção contra a constituição e a exploração de ficheiros que não estejam conformes com as disposições da presente directiva. Para este efeito, disporá, nomeadamente do direito de acesso aos ficheiros abrangidos pela presente directiva, devendo poder recolher quaisquer informações necessárias ao cumprimento da suas funções de controlo.

3. A referida autoridade podem ser apresentadas por qualquer pessoa denúncias ou reclamações relativas à protecção das pessoas no que diz respeito a dados pessoais.

Artigo 27º

Grupo de protecção dos dados pessoais

1. É criado um Grupo de protecção dos dados pessoais. O Grupo, de natureza consultiva e independente, será composto por representantes da autoridade de controlo, prevista no artigo 26º, de todos os Estados-membros e presidido por um representante da Comissão.

2. O secretariado do Grupo de protecção dos dados pessoais será assegurado pelos serviços da Comissão.

3. O Grupo de protecção dos dados pessoais elaborará o seu regulamento interno.

4. O Grupo de protecção dos dados pessoais apreciará as questões introduzidas na ordem de trabalhos pelo seu Presidente, quer por iniciativa deste quer a pedido fundamentado de um representante das autoridades de controlo, e que digam respeito à aplicação das disposições de direito comunitário em matéria de protecção de dados pessoais.

Artigo 28º

Atribuições do Grupo de protecção dos dados pessoais

1. O Grupo de protecção dos dados pessoais tem as seguintes atribuições:

   a) contribuir para a aplicação homogénea das regras nacionais de execução da presente directiva;

   b) emitir parecer sobre o nível de protecção na Comunidade e nos países terceiros;

   c) aconselhar a Comissão sobre projectos de medidas adicionais ou específicas a tomar para salvaguardar a protecção da vida privada.

2. Se o Grupo de protecção dos dados pessoais verificar que surgem graves divergências entre a legislação ou a prática dos Estados-membros em matéria de protecção dos dados pessoais que ameacem prejudicar a equivalência da protecção na Comunidade, informará a Comissão desse facto.

3. O Grupo de protecção dos dados pessoais pode emitir recomendações sobre todas as questões relativas à protecção das pessoas no que diz respeito aos dados pessoais na Comunidade. As recomendações constarão da acta e podem ser transmitidas ao Comité Consultivo a que se refere o artigo 30º. A Comissão informará o Grupo de protecção dos dados pessoais do seguimento que deu às recomendações.

4. O Grupo de protecção dos dados elaborará um relatório anual sobre a situação da protecção das pessoas relativamente ao tratamento dos dados pessoais na Comunidade e nos países terceiros.

CAPÍTULO X

PODER REGULAMENTAR DA COMISSÃO

Artigo 29º

Exercício do poder regulamentar

A Comissão adoptará, de acordo com o processo previsto no nº 2 do artigo 30º, as modalidades de carácter técnico necessárias para aplicar a presente directiva às especificidades de certos sectores, tendo em conta a situação nesta matéria e os códigos de boa conduta.

Artigo 30º

Comité Consultivo

1. A Comissão será assistida por um Comité consultivo composto por representantes dos Estado-membros e presidido pelo representante da Comissão.

2. O representante da Comissão apresentará ao Comité um projecto de medidas a tomar. O Comité emitirá um parecer sobre este projecto, num prazo que o presidente pode fixar em função da urgência da questão em causa, se necessário procedendo a uma votação. O parecer constará da acta; além disso, cada Estado-membro terá o direito de solicitar que a sua posição conste dessa mesma acta. A Comissão tomará na melhor conta o parecer emitido pelo Comité. O Comité será por ela informado do modo como tomou em consideração o seu parecer.

DISPOSIÇÕES FINAIS

Artigo 31o

1. Os Estados-membros adoptarão as disposições legislativas, regulamentares e administrativas necessárias para darem cumprimento à presente directiva, o mais tardar até 1 de Janeiro de 1993.

   As disposições adoptadas por força do nº 1 referir-se-ão explicitamente à presente directiva.

2. Os Estados-membros comunicarão à Comissão o texto das disposições de direito interno que venham a adoptar no domínio regulado pela presente directiva.

Artigo 32o

A Comissão transmitirá periodicamente ao Conselho e ao Parlamento Europeu um relatório sobre a aplicação da presente directiva nele incluindo, se for caso disso, propostas de alteração adequadas.

Artigo 33o

Os Estados-membros são os destinatários da presente directiva.

Feito em Bruxelas, em

Pelo Conselho

Fiche Financière

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL VISANT AU RAPPROCHEMENT DE CERTAINES DISPOSITIONS LEGISLATIVES, REGLEMENTAIRES ET ADMINISTRATIVES DES ETATS MEMBRES RELATIVES A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1. Ligne budgétaire concernée (éventuellement à créer) :

   A 2511 : Frais de réunions de comités dont la consultation n'est pas un élément obligatoire de la procédure de formation d'actes communautaires.

2. Base légale (ou autre) :

   Article 100 A

3. Proposition de classification en dépense obligatoire/non obligatoire

   (avec justification succincte en vertu de la déclaration commune du 30 juin 1982) :
   non-obligatoire

4. Description et justification de l'action :

   4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,
   - permettre la circulation transfrontière de données à caractère personnel dans la Communauté,
   - permettre le bon fonctionnement du marché intérieur.

   4.2. Création de 2 comités compétents en matière de protection des personnes à l'égard des données à caractère personnel (Art. 27,30)

   personnes concernées : 1. Pour le Comité de protection des données à caractère personnel (Art. 27) : représentants de l'autorité de contrôle de tous les Etats membres (groupe 4)

   2. Pour le Comité consultatif (Art.30) : représentants des Etats membres (groupe 3)

   4.3. Un représentant de la Commission préside le Comité de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions
(frais de participation des membres des 2 Comités)

5.2. Calcul : - Comité de protection des données :
24 membres (non-gouvernementals) x 3 réunions
a 2 jours x 1180 ECU (590 ECU/jour) = 84.960 ECU*
- Comité consultatif :
24 membres (gouvernemental) x 1 réunion a 2 jours x
780 ECU (390 ECU/jour) = 18.720 ECU*

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

	CE-CP
1993 :	103.680 ECU
1994 :	" "
1995 :	" "
1996 :	" "
1997 :	" "

6.2. Part du financement communautaire dans le coût total : 100%

7. Observations :

1. Le Comité de protection des données à caractère personnel (Art. 27) :

Il est institué ce Comité à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tout les Etats membres, présidé par un représentaht de la Commission.

Ce Comité établit son règlement intérieur. Le secrétariat du Comité est assuré par les services de la Commission.

Missions de ce Comité : voir Art.28.

2. Le Comité consultatif (Art.30) :

Il est institué un Comité consultatif composé des représentants des Etats membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de cèrtaines secteurs.

---

* estimation

FICHE D'IMPACT SUR LA COMPETITIVITE ET L'EMPLOI

I. Quelle est la justification principale de la mesure ?

- Assurer la protection des personnes à l'égard des données à caractère personnel.

- Permettre la circulation transfrontière de données à caractère personnel dans la Communauté.

- Permettre le bon fonctionnement du marché intérieur.

II. Caractéristiques des entreprises concernées.

La proposition concerne toutes les entreprises qui utilisent des fichiers de données à caractère personnel quel que soit leur taille ou leur secteur d'activité.

III. Quelles sont les obligations imposées directement aux entreprises ?

Se conformer aux dispositions applicables aux traitements de données à caractère personnel, notamment celles relatives à la légitimité de ces traitements dans le secteur privé.

IV. Quelles sont les obligations susceptibles d'être imposées indirectement aux entreprises via les autorités locales ?

Aucune.

V. Y a-t-il des mesures spéciales pour les PME ?

Non.

VI. Quel est l'effet prévisible ?

a) sur la compétitivité des entreprises ?

Les règles de protection s'appliquent à toutes les entreprises et élimineront les distorsions de concurrence dûes à l'actuelle disparité des législations nationales. En ce qui concerne leur compétitivité internationale, la directive prévoit des négociations avec les pays tiers qui n'assurent pas encore un niveau de protection adéquat.

b) sur l'emploi ?

La directive prévoit la création d'instances de contrôle nationales.

VII. Les partenaires sociaux ont-ils été consultés sur cette proposition ?

Non.

Projecto de

RESOLUÇÃO DOS REPRESENTANTES DOS GOVERNOS DOS ESTADOS-MEMBROS DAS COMUNIDADES EUROPEIAS REUNIDOS EM CONSELHO

Os Representantes dos Governos dos Estados-membros das Comunidades Europeias reunidos em Conselho,

Considerando que a Directiva do Conselho relativa à aproximação de certas disposições legislativas, regulamentares e administrativas dos Estados-membros respeitantes à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais assegura a protecção da vida privada das pessoas relativamente ao tratamento dos dados pessoais contidos em ficheiros do sector privado e do sector público, excluindo ficheiros do sector público cujas actividades não relevem do âmbito do direito comunitário;

Desejosos de facilitar a cooperação entre as Administrações dos Estados-membros nos sectores que não relevam do âmbito do direito comunitário assegurando simultaneamente um alto nivel de protecção da vida privada das pessoas afectadas;

Considerando que os principios constantes da directiva concretizam e ampliam os da Convenção de 28 de Janeiro de 1981 do Conselho da Europa relativa à protecção das pessoas no que diz respeito do tratamento automatizado dos dados pessoais;

Acordaram na seguinte resolução:

Os Governos dos Estados-membros comprometem-se a aplicar os principios constantes da Directiva do Conselho relativa à aproximação de certas disposições legislativas, regulamentares e administrativas dos Estados-membros respeitantes à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais ao sector público não abrangido no âmbito do direito comunitário, e a dar inicio aos processos legislativos necessários para o efeito.

DECLARAÇÃO DA COMISSÃO

relativa à aplicação às instituições e organismos das Comunidades Europeias dos princípios da Directiva relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais

1. A Comissão considera que os princípios da Directiva relativa à protecção das pessoas no que diz respeito aos dados pessoais ("a directiva") devem ser aplicados às instituições e organismos das Comunidades Europeias.

2. Para este efeito, a Comissão tomará e proporá, o mais rapidamente possível, as medidas necessárias.

3. Na pendência de que estas medidas sejam tomadas, a Comissão compromete-se a aplicar os princípios constantes da directiva aos tratamentos dos dados pessoais que relevam da sua competência.

4. A Comissão considera que as outras instituições das Comunidades se devem comprometer igualmente a aplicar os princípios constantes da directiva aos tratamentos de dados pessoais que relevam da sua competência.

SYN 288

Proposta de

DIRECTIVA DO CONSELHO

relativa à protecção de dados pessoais e da vida privada no contexto das redes públicas digitais de telecomunicações, nomeadamente a rede digital de serviços integrados (RDSI) e as redes públicas móveis digitais

---

TABLE DES MATIERES

A RESUME .....

B EXPOSE DES MOTIFS .....

I Introduction .....

II Les nouvelles exigences relatives à la protection des données personnes et de la vie privée dans le secteur des télécommunications. .....

III La démarche proposée - les dispositions du projet de directive .....

IV Conclusions .....

PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLIQUES, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES MOBILES PUBLICS

A. RESUME

L'introduction des réseaux numériques publics de télécommunications a maintenant atteint sa phase de concrétisation dans toute la Communauté. Au cours des premières années de cette décennie, plus de 70 % des transmissions à grande distance, de 50 % des commutations à grande distance et de 30 % des commutations locales seront numérisées.

L'introduction généralisée des réseaux numériques publics de télécommunications dans la Communauté permettra, notamment grâce à la mise en oeuvre du réseau numérique à intégration de services (RNIS) et des nouveaux services numériques mobiles, d'offrir au grand public des fonctions de télécommunications très largement améliorées mais exigera dans un même temps une approche commune à l'échelle communautaire en matière de protection de la vie privée, des données à caractère personnel et de la sécurité des données, eu égard aux exigences spécifiques du nouvel environnement des télécommunications numériques.

Le Conseil et le Parlement européen ont à diverses reprises souligné le rôle central que doivent jouer les mesures appropriées de protection des données et de la vie privée pour le développement futur des télécommunications dans la Communauté européenne. Dans sa résolution du 14 décembre 1988 sur les télécommunications, le Parlement européen a en particulier préconisé des mesures spécifiques "visant à assurer la protection des données et à garantir la confidentalité" et rappelé à la Commission "qu'il relève de sa responsabilité politique, parallèlement à la présentation de textes législatifs visant à ouvrir les marchés des télécommunications, de veiller à ce que des initiatives soient prises, sous les formes juridiques appropriées, pour assurer la protection des données à caractère personnel" dans la Communauté.

Dans la Communauté, on attache une attention de plus en plus importante à l'impact des réseaux numériques sur la protection des données à caractère personnel et de la vie privée. Dans une résolution adoptée à Berlin en 1989, les responsables de la protection des données dans les Etats membres ont demandé qu'une attention particulière soit accordée à la protection des données à caractère personnel et de la vie privée dans le contexte du RNIS.

La proposition jointe au présent document vise à répondre aux exigences spécifiques concernant la protection des données à caractère personnel et de la vie privée dans le domaine des nouveaux réseaux numériques publics de télécommunications. Cette proposition est présentée dans le contexte des propositions de la Commission, et complète ces dernières, concernant l'établissement d'un cadre général pour la protection des données dans la Communauté.

La protection effective des données à caractère personnel et de la vie privée devient une condition préalable essentielle à l'acceptation sociale des nouveaux réseaux et services numériques. Elle doit constituer un élément fondamental de la politique communautaire des télécommunications qui a pour but d'offrir au citoyen européen tous les avantages des services avancés de télécommunications, à un moment où la Communauté s'oriente vers un environnement qui sera sensiblement plus riche en informations que par le passé.

La proposition de directive du Conseil ci-jointe a été élaborée dans la perspective de cet objectif général.

B. EXPOSE DES MOTIFS

I. Introduction

La phase actuelle d'introduction généralisée des télécommunications numériques publiques dans la Communauté, et en particulier la mise en oeuvre du réseau numérique à intégration de services (RNIS)[1] et des nouveaux services numériques mobiles[2] doit permettre d'offrir au grand public des fonctions de télécommunications très largement améliorées mais, dans un même temps, exigera une approche commune à l'échelle européenne en matière de protection de la vie privée, des données à caractère personnel et de la sécurité des données eu égard aux exigences spécifiques du nouvel environnement de télécommunications numériques.

Dans sa résolution concernant l'introduction coordonnée du réseau numérique à intégration de services dans la Communauté européenne du 12 décembre 1986[3], le Parlement européen a précisé que "dans le cadre du développement du réseau téléphonique le futur réseau numérique à intégration de services (RNIS) offrira un grand nombre de services supplémentaires aux usagers professionnels et privés..." mais a invité la Commission "à présenter des propositions permettant d'assurer judicieusement, dans le cadre du réseau RNIS en voie de création, un niveau de protection des données uniforme et adapté aux possibilités techniques accrues du nouveau système". Le Parlement européen a ensuite repris et développé ce thème dans un contexte plus général, dans le cadre de sa résolution du 14 décembre 1988[4] où il préconise des mesures spécifiques concernant l'utilisation des réseaux de télécommunications "visant à assurer la protection des données et à garantir la vie privée" et rappelé à la Commission "qu'il relève de sa responsabilité politique, parallèlement à la présentation de textes législatifs visant à ouvrir les marchés des télécommunications, de veiller à ce que des initiatives soient prises, sous les formes juridiques appropriées, pour assurer la protection des données à caractère personnel" dans la Communauté.

---

(1) Recommandation du Conseil du 22 décembre 1986 concernant l'introduction coordonnée du réseau numérique à intégration de services (RNIS) dans la Communauté européenne (86/659/CEE).
Le RNIS peut être considéré comme une évolution naturelle du réseau téléphonique. Il permettra la transmission, via un accès unique et les lignes d'abonnés existantes, de signaux vocaux (téléphonie) de textes, de données et d'images sous la forme de toute une série de services plus efficaces ou nouveaux (pour plus de détails voir la recommandation du Conseil 86/659/CEE et le chapitre II).
Conformément à la recommandation du Conseil, deux rapports sur l'état d'avancement de la mise en oeuvre du RNIS ont été présentés jusqu'à présent par la Commission (COM(88)589; COM(90)123).

(2) Recommandation du Conseil du 25 juin 1987 concernant l'introduction coordonnée des communications mobiles terrestres publiques cellulaires numériques paneuropéennes dans la Communauté (87/371/CEE, JO L 196 du 17 juillet 1987, p. 81) et directive du Conseil du 25 juin 1987 relative aux bandes de fréquence à réserver pour l'introduction coordonnée des communications mobiles terrestres publiques cellulaires numériques paneuropéennes dans la Communauté (87/372/CEE, JO L 196du 17 juillet &987, p. 85), et propositions ultérieures de la Commission dans le domaine des communications numériques mobiles publiques.

(3) Résolution sur la recommandation du Conseil 86/659/CEE, JO C 7 du 12 janvier 1987, p. 334.

(4) Résolution sur les postes et télécommunications, JO C 12 du 16 janvier 1989, p. 69 ; résolution sur la nécessité de résoudre le problème de fragmentation des télécommunications, JO C 12 du 16 janvier 1989, p. 66.

Le Conseil, dans sa résolution du 30 juin 1988[5] par laquelle il a adopté les principes du Livre vert sur le développement du Marché commun des services et équipements des télécommunications[6] et a accordé son soutien général aux objectifs du programme d'action fixés dans la communication du 9 février 1988[7] a considéré que l'un des objectifs politique majeurs était "de protéger les données à caractère personnel et de donner à chaque personne accès, grâce aux moyens de communication, à un environnement sensiblement plus riche en informations".

Dans sa résolution sur le renforcement de la coordination pour l'introduction du réseau numérique à intégration de services (RNIS) dans la Communauté européenne pour 1992[8] le Conseil a développé ce thème, dans la perspective du RNIS, en soulignant qu'il était nécessaire de poursuivre "la discussion au niveau européen sur les exigences de la protection de la vie privée des utilisateurs et les exigences en matière de sécurité des communications dans le contexte de la forunitures de nouveaux services, conformément à la résolution du Parlement européen du 12 décembre 1986 sur la recommandation 86/659/CEE".

Les représentants des autorités de contrôle responsables de la protection des données dans les Etats membres ont adopté lors de la 11e Conférence internationale tenue à Berlin du 28 au 31 août 1989 une résolution demandant qu'une attention particulière soit accordée à la protection des données et la vie privée dans le contexte du RNIS.

La Commission, par la proposition jointe au présent document, répond à ces exigences en matière de mesures communautaires spécifiques concernant la protection des données à caractère personnel et de la vie privée dans le contexte de la mise en oeuvre des nouveaux réseaux numériques publics de télécommunications, et en particulier du réseau numérique à intégration de services et des réseaux numériques mobiles publics. Elle tient compte du climat de préoccupation - parfaitement fondé - concernant l'impact immédiat des réseaux numériques sur la protection des données à caractère personnel et de la vie privée. La Commission a également considéré que la protection des données et la protection de la vie privée constituent des exigences essentielles dans le contexte du développement futur d'un environnement de réseau ouvert dans la Communauté[9]

---

(5) Resolution du Conseil du 30 juin 1988 sur le développement du Marché commun des services et équipements des télécommunications d'ici à 1992 (JO C 257, p. 1).

(6) COM(87)290.

(7) Vers un marché communautaire concurrentiel des télécommunications 1992 - mise en oeuvre du Livre vert sur le développement du Marché commun des services et équipement de télécommunications. Etat des discussions et propositions de la Commission (COM(88)48).

(8) JO C 196 du 1er août 1989, p. 4

(9) Position commune arrêtée par le Conseil le 5.2.1990 en vue de l'adoption de la Directive relative à l'établissement du marché intérieur des services de telecommunications par la mise en oeuvre de la fourniture de réseau ouvert de télécommunications, J.O. ...

La proposition doit être envisagée dans le contexte des discussions et des principes généraux concernant la protection des données à caractère personnel établis en Europe par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et qui a été ratifié à l'heure actuelle par sept Etats membres de la Communauté. La proposition esr présentée dans le contexte des propositions de la Commission, et complète ces dernières, concernant l'établissement d'un cadre général pour la protection des données dans la Communauté qui sont soumises parallèlement, et en particulier du projet de proposition de directive du Conseil visant au rapprochement de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la protection des personnes à l'égard du traitement des données à caractère personnel, le projet de recommendation d'une décision du Conseil concernant l'ouverture des négociations en vue de l'adhésion de la Communauté économique européenne, dans les domaines qui sont de sa compétence, à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la proposition de Décision du Conseil dans le domaine de la sécurité des systèmes de l'information ; en complément, la Commission développera des règles internes visant à garantir aux personnes concernées un niveau de protection équivalent aux principes de la Directive du Conseil mentionnée ci-dessus.

Dans ce contexte général, la directive ci-jointe a pour objectif de prévoir les dispositions requises pour le rapprochement des législations, réglements et dispositions administratives dans la Communauté dans le domaine de la protection des données à caractère personnel et de la vie privée, eu égard aux réseaux numériques mobiles et fixes de télécommunications publics et aux nouvelles fonctions "intelligentes" qu'ils offrent.

II. Les nouvelles exigences spécifiques concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications

La "numérisation" des réseaux publics de télécommunications est maintenant en cours dans l'ensemble de la Communauté. Au cours des premières années de cette décennie, plus de 70 % des transmissions à grande distance, 50 % des commutations à grande distance et 30 des commutations locales seront numérisées.

Le concept de numérisation porte sur l'introduction de centraux entièrement informatisés et sur le traitement et la transmission de toutes les informations circulant via les réseaux de télécommunications - signaux vocaux, données et images - sous la forme de chiffres binaires[10]. Les "trains binaires" ainsi produits peuvent être traités directement grâce à l'intelligence des ordinateurs, tant à l'intérieur du réseau que dans le terminal de l'abonné. Cette technique débouche sur des services d'un niveau qualitatif accru qui ne peut être obtenu avec les techniques "analogiques" traditionnelles, ainsi que sur un nombre important de nouvelles fonctions "intelligentes" ouvrant une vaste gamme de nouvelles activités via les réseaux de télécommunications. Les communications entièrement numérique d'un point à l'autre (abonné à abonné) sont offertes par le réseau numérique à intégration de services en évolution et les nouveaux systèmes de communications mobiles publiques numériques[11].

Pour ce qui concerne la protection de données, l'introduction des réseaux numériques publics a deux conséquences essentielles.

D'une part, les techniques entièrement informatisées qui peuvent aujourd'hui être utilisées permettent d'offrir un niveau nettement plus élevé de sécurité des données en fonction d'exigences individuelles spécifiques, grâce par exemple aux techniques perfectionnées de chiffrement.

D'autre part, en raison du traitement numérique des données de fonctionnement et d'appel, et du traitement par les centraux informatisés, il deviendrait possible - en l'absence de mesures adéquates de protection des données - de stocker et de surveiller systématiquement les données spécifiques relatives aux appels, concernant notamment leur origine. De tels contrôles n'étaient possibles dans les réseaux traditionnels analogiques "non intelligents" que par la mise en oeuvre d'efforts techniques considérables et ils n'étaient donc utilisé que dans des circonstances tout à fait exceptionnelles

Dans, un même temps, les nouvelles fonctions intelligents de télécommunications, telles qu'elles sont définies par les "services supplémentaires" du RNIS[12] offrent à l'abonné des fonctions de services supplémentaires, du type facturation détaillée, non négligeables qui amélioreront la qualité des services ainsi que la protection des consommateurs. Les nouvelles fonctions exigeront cependant des mesures et réglementations particulières, si l'on veut garantir dans le nouvel environnement la protection de la vie privée.

---

(10) Les ordinateurs traitent toutes les informations sous la forme de "chiffres binaires", c'est-à-dire en fragmentant toutes les informations en éléments d'information fondamentaux (bits) de valeurs zéro ou un.

(11) Voir les recommandations du Conseil 86/659/CEE et 87/371/CEE, notes en bas de page 1 et 2 ci-avant.

(12) Pour plus de détails, voir la recommandation du Conseil 86/659/CEE, note N°1

Par conséquent, l'introduction des réseaux numériques de télécommunications dans la Communauté suscite, en matière de protection des données à caractère personnel, des questions importantes qui doivent être abordées, notamment en matière de traitement :

- des informations concernant l'abonné, de plus en plus souvent stockées dans des fichiers informatisés d'abonnés ;
- des données relatives au trafic et à d'autres fonctions opérationnelles ;
- des données relatives à la facturation détaillée;
- de l'identification de la ligne appelante ;
- du renvoi automatique d'appels à des tiers;
- des messages non sollicités;
- des caractéristiques techniques spécifiques pour les terminaux et autres équipements qui peuvent être requises afin d'assurer une protection appropriée.

Les mesures générales de protection des données à caractère personnel, du type préconisé par la Convention du Conseil de l'Europe et qui doivent être établies par la Communauté, par le truchement des initiatives de la Commission citées ci-avant, constituent un cadre général mais ne prévoient aucune disposition concernant les mesures détaillées requises pour aborder ces questions.

Les dispositions générales relatives à la protection des données à caractère personnel ne peuvent empêcher à l'heure actuelle l'apparition de législations, réglementations et mesures administratives divergentes dans les Etats membres pour ce qui concerne l'exploitation des futurs réseaux numériques qui pourraient très rapidement menacer le développement du marché commun des services et équipements terminaux de télécommunications.

Ainsi, dans le domaine de l'identification de la ligne appelante, certains Etats membres prévoient une élimination cas par cas de cette fonction par l'abonné appelant. Dans le cas où une telle élimination se ferait à l'aide d'un bouton sur le combiné téléphonique, tandis que d'autres exploitants décideraient de prévoir cette élimination à l'aide d'un code à utiliser avant le lancement de l'appel, la libre circulation de équipements terminaux dans la Communauté deviendrait problématique.

Une comparaison établie entre les dispositions nationales existantes révèle des divergences considérables concernant à la fois la teneur et la nature des instruments juridiques utilisés. Dans ces circonstances, on voit se développer dans la Communauté une situation d'incertitude juridique en ce qui concerne les réseaux et services de télécommunications, incertitude qui fait peser une lourde menace sur l'offre transfrontière de services.

En l'absence d'une directive concernant les mesures spécifiques requises pour mettre en oeuvre les principes généraux de protection des données et de la vie privée, dans le contexte des réseaux numériques fixes et mobiles publics, il serait impossible d'empêcher des développements divergents dans la Communauté.

Dans un même temps, la protection effective à l'échelle communautaire des données à caractère personnel et de la vie privée devient une condition préalable essentielle à l'acceptation sociale des nouveaux réseaux et services numériques; cette exigence a été confirmée par le Conseil lors de sa réunion du 7 novembre 1989 où il a conclu, en ce qui concerne les aspects sociaux des télécommunications, qu'il était indispensable d'assurer la protection de la vie privée et des données à caractère personnel dans une perspective européenne.

La proposition de directive du Conseil jointe au présent document a pour objectif de répondre à ces exigences spécifiques.

III. La démarche proposée : les dispositions du projet de directive

L'objectif général de la proposition de directive est de garantir au citoyen européen dans l'ensemble de la Communauté un niveau de base de protection des données à caractère personnel et de la vie privée, par des mesures qui doivent être intégrées dans l'offre générale des nouvelles télécommunications numériques, tout en renvoyant les exigences relatives aux niveaux améliorés de sécurité des données pour des cas et applications individuels précis aux mesures spécifiques qui doivent être mises au point dans le cadre du programme de travail fixé par la proposition de la Commission de décision du Conseil concernant la sécurité des systèmes d'information citée ci-dessus.

La directive proposée vise à établir un niveau de base de protection de l'abonné en général dans le nouvel environnement numérique en soulignant deux principes fondamentaux :

- minimiser le risque d'abus en limitant les données traitées et stockées dans le contexte de l'exploitation des télécommunications publiques au strict minimum requis pour assurer un niveau adéquat de l'exploitation, la qualité du service et les fonctions offertes à l'abonné ;

- garantir pleinement à l'abonné le droit d'autodétermination en matière d'information, tant en ce qui concerne l'organisation des télécommunications fournissant les services qu'à l'égard de l'autre abonné dans l'établissement d'une connexion et de tout tiers qui pourrait vouloir obtenir un accès aux données transmises ou fournies dans le contexte d'une transaction via un réseau public de télécommunications.

Comme l'impact le plus marqué sur l'abonné en général du nouvel environnement de télécommunications portera sur le domaine de la téléphonie vocale, la directive proposée est centrée sur ce secteur. Toutefois, elle prévoit une procédure concernant l'application des dispositions relatives à la téléphonie vocale à d'autres services de télécommunications publiques numériques, le cas échéant, comme les services publics de transmission de données dans le contexte du R.N.I.S., les réseaux de données à commutation de paquets et de circuits et d'autres services de télécommunications publiques connexes.

En outre, au vue de l'état actuel de transition des réseaux publics de télécommunication dans la Communauté, et en particulier du fait que certains centraux à commande par programmes stockés (SPC), bien qu'ils ne soient pas encore numériques, fournissent un certain nombre des fonctions intelligentes concernées, la directive proposée prévoit, dans le cas où un Etat membre n'a pas encore mis en oeuvre le réseau numérique à intégration de service ou les réseaux numériques mobiles publics, que les dispositions de la directive seront mises en oeuvre dans la mesure où elles s'appliquent également aux services basés sur des réseaux analogiques.

Compte tenu de ces principes généraux, la teneur de la directive proposée aborde plus particulièrement : la collecte, le stockage et le traitement des données à caractère personnel dans le fichier de l'abonné; le stockage et le traitement des données relatives au trafic et à la facturation, en particulier aux fins de l'établissement d'une facturation détaillée; le problème de l'identification de la ligne appelante ; l'accès par des tiers, les appels non sollicités; et les procédures qui doivent être adoptées afin d'établir les normes techniques déterminées qui pourrait être requise.

Les articles de la Directive sont brièvement expliqués ci-dessous :

Les articles premier et 2 décrivent les objectifs généraux de la directive et son application à la protection des données et de la vie privée, eu égard aux services publics de télécommunication dans les réseaux numériques publics de télécommunications dans la Communauté.

L'article 3 contient les définitions des termes importants, dans la ligne de la position commune du Conseil relative à la mise en oeuvre de la fourniture d'un réseau ouvert (ONP) mentionnée ci-dessus [13].

Le principe général de l'article 4 selon lequel la collecte, le stockage et le traitement des données à caractère personnel par une organisation des télécommunications se justifient uniquement aux fins de la fourniture du service voulu et ne peuvent être utilisés sans autorisation légale ou sans consentement préalable de l'abonné à d'autres fins est appliqué dans l'article 5 à la création de fichiers d'abonnés. Comme le précise l'introduction de la directive, ces opérations de collectes, de stockage et de traitement des données à caractère personnel ne peuvent en particulier être utilisées pour donner à une organisation des télécommunications un avantage concurrentiel quelconque indu vis-à-vis d'autres prestataires de service dans des domaines concurrentiels.

L'article 6 énumère les droits de l'utilisateur concernant ses données à caractère personnel détenues par une organisation des télécommunications et l'article 7 précise le principe de non divulgation de ces données à des tiers sans le consentement de l'abonné ou une autorisation légale.

L'article 8 a pour but de garantir un niveau adéquat de protection des données contre tout accès non autorisé.

Les articles 9 et 10 appliquent le principe du stockage et du traitement des données à caractère personnel dans la mesure requise à des fins de télécommunication, uniquement aux données relatives à la facturation et au trafic. L'aticle 11 a pour but de protéger la vie privée des abonnés pour ce qui concerne la facturation détaillée, via l'exigence d'anonymat de l'abonné appelant.

Les articles 12 et 13 contiennent les dispositions détaillées relatives à l'identification de la ligne appelante. La possibilité d'éliminer cette fonction d'identification doit être disponible parce que, entre autres, les appelants en liaison téléphonique avec des centres de réhabilitation de drogués et d'alcooliques, des centres de protection de la famille ou des services de santé mentale sont légitimement préoccupés par le fait que cette caractéristique du service téléphonique pourrait compromettre leur anonymat; la même remarque s'applique aux lignes téléphoniques d'aide à la prévention du suicide et en matière de SIDA.

Toutefois, l'abonné appelé peut avoir un intérêt légitime à recevoir uniquement des appels identifiés. Afin de garantir le droit à l'autodétermination de l'information tant à l'appelant qu'à l'appelé, l'abonné appelé doit donc avoir la possibilité de limiter l'acceptation des appels entrants à ceux qui identifient le numéro de l'abonné appelant.

De plus, les organisations de télécommunications doivent fournir une fonction d'annulation (blocage) de l'élimination de la fonction d'identification en cas d'appels malveillants; la fonction doit également pouvoir être disponible à des fins de poursuite de délits criminels et pour les services d'urgence en particulier pour les brigades de pompiers, afin d'empêcher l'abus de services de ce type.

L'article 14 assure la protection de la vie privée et de l'abonné appelant et de l'abonné appelé en cas d'utilisation des fonctions de renvoi d'appel.

L'article 15 a pour but d'empêcher, par des moyens techniques que le contenu des appels téléphoniques soit stockée et/ou diffusée à des tiers sans information préalable de l'abonnée appelant.

---

13) voir note N° 9.

Les articles 16 et 17 visent à empêcher l'utilisation non autorisée des données à caractère personnel des abonnés par les prestataires de services de télé-achat et vidéotex afin d'éviter l'établissement de profils de consommateurs; ils visent également à la protection de la vie privée des abonnés contre les messages non sollicités, comme par exemple la publicité indésirable via des moyens de télécommunication.

L'article 18 a pour but d'empêcher que l'introduction de fonctions techniques basées sur des exigences de protection des données puisse entraîner l'apparition de restrictions indues à la libre circulation des équipements et services de télécommunications dans la Communauté, en assurant, si nécessaire, l'élaboration de normes européennes communes concernant la mise en oeuvre de fonctions techniques spécifiques. Conformément à la directive du Conseil sur le rapprochement des législations des Etats membres relatives aux équipements terminaux de télécommunications, incluant la reconnaissance mutuelle de leur conformité [14], et à la décision du Conseil 87/95/CEE du 22 décembre 1986 sur la normalisation dans le domaine des technologies de l'information et des télécommunications [15], des travaux techniques doivent être confiés aux organismes européens de normalisation adéquats, et en particulier à l'Institut européen des Normes de Télécommunication (ETSI) et au CEN/CENELEC.

Les dispositions finales des articles 19 à 25 portent sur le champ d'application des modifications requises pour adapter cette directive aux nouveaux développements techniques et les procédures de consultation. Il est prévu qu'un groupe composé de représentants des autorités de contrôle responsables de la protection des données dans les Etats membres et qu'un comité composé de représentant des Etats membres assistent la Commission dans la mise en oeuvre de la directive. Ces comités devraient être, selon la proposition, ceux définis à cette fin dans le projet de proposition de directive du Conseil visant au rapprochement de certaines dispositions législatives, réglementaires et administratives des Etats membres relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui est présenté parallèlement(voir ci-dessus) mais seraient institués spécifiquement aux fins de la présente directive.

---

(14) COM(89)289 - SYN 204, 27.7.1989

(15) J.O. L36, 7 février 1987, p. 31

IV. Conclusion

La protection effective à l'échelle communautaire des données à caractère personnel et de la vie privée devient une condition préalable essentielle à l'acceptation sociale des nouveaux réseaux et services numériques.

En l'absence d'une directive concernant les dispositions spécifiques requises pour mettre en oeuvre les principes généraux de protection des données à caractère personnel et de la vie privée, eu égard aux exigences spécifiques des réseaux numériques fixes et mobiles publics, il serait impossible d'empêcher des développements divergents dans la Communauté qui menaceraient rapidement le développement du marché commun des services et équipements terminaux de télécommunications.

Le projet de directive ci-joint a pour but de prévoir ces dispositions spécifiques.

Le Conseil est par conséquent invité à adopter la proposition de directive jointe au présent document.

SYN 288

Proposta de

DIRECTIVA DO CONSELHO

relativa à protecção de dados pessoais e da vida privada no contexto das redes públicas digitais de telecomunicações, nomeadamente a rede digital de serviços integrados (RDSI) e as redes públicas móveis digitais

---

O CONSELHO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Económica Europeia e, nomeadamente, o seu artigo 100º A,

Tendo em conta a proposta da Comissão(1)

Em cooperação com o Parlamento Europeu(2)

Tendo em conta o parecer do Comité Económico e Social(3)

1. Considerando que a Directiva ... do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais preconiza que os Estados-membros assegurem a protecção da vida privada das pessoas;

2. Considerando que estão a surgir actualmente na

---

(1) ...

(2) ...

(3) ...

Comunidade Europeia novas redes públicas telefónicas digitais avançadas que suscitam requisitos específicos relativos à protecção de dados pessoais e da vida privada do utilizador;

3. Considerando que esta questão está especialmente relacionada com a introdução da Rede Digital de Serviços Integrados (RDSI) e de redes públicas móveis digitais;

4. Considerando que o Conselho de Ministros, na sua Resolução de 30 de Junho de 1988 relativa ao desenvolvimento do mercado comum de serviços e equipamentos de telecomunicações até 1992(4), apelava para a tomada de medidas destinadas à protecção de dados pessoais, a fim de ser criado um ambiente adequado para o futuro desenvolvimento das telecomunicações na Comunidade; que o Conselho voltou a sublinhar a importância da protecção de dados pessoais e da vida privada na sua Resolução de 18 de Julho de 1989 relativa ao reforço da coordenação para a introdução da Rede Digital de Serviços Integrados (RDSI) na Comunidade Europeia (5);

5. Considerando que o Parlamento Europeu sublinhou a importância da protecção de dados pessoais e da vida privada nas redes de telecomunicações, nomeadamente no que respeita à introdução da Rede Digital de Serviços Integrados (RDSI)(6)(7)(8);

6. Considerando que a Recomendação 81/679/CEE da Comissão

---

(4) JO nº C 257 de 4.10.1988, p. 1.
(5) JO nº C 196 de 1.8.1989, p. 4.
(6) JO nº C 7 de 12.1.1987, p. 334.
(7) JO nº C 12 de 16.1.1989, p. 69.
(8) JO nº C 12 de 16.1.1989, p. 66.

de 29.7.1981 faz apelo à adopção e ratificação pelos Estados-Membros da Convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, que enuncia princípios gerais para a protecção de dados pessoais;

7. Considerando que diversos Estados-membros adoptaram e ratificaram esta Convenção;

8. Considerando que a Directiva ..... (CEE) (9) do Conselho prevê a abertura de negociações com vista à adesão da Comunidade Económica Europeia, nos domínios que são da sua competência, à Convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal

---

(9) JO ...

9. **Considerando que a Directiva .....**(CEE) do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais põe em prática a adopção destes princípios gerais na Comunidade;

10. **Considerando que, no caso das redes públicas digitais, é necessário estabelecer disposições legislativas, regulamentares e técnicas específicas para protecção dos dados pessoais e da vida privada dos utilizadores face aos riscos crescentes que podem estar ligados ao armazenamento e tratamento informático de dados pessoais naquelas redes;**

11. Considerando que os Estados-membros estão actualmente a desenvolver disposições divergentes nesta área;

12. Considerando que, dados os obstáculos resultantes daquelas disposições legislativas, regulamentares e técnicas divergentes respeitantes à protecção de dados pessoais e da vida privada no contexto da implantação de redes públicas digitais de telecomunicações na Comunidade, nomeadamente a Rede Digital de Serviços Integrados (RDSI) e as redes públicas móveis digitais, o pleno estabelecimento de um mercado comunitário de serviços e equipamentos de telecomunicações exige a rápida introdução de disposições harmonizadas;

13. Considerando que a presente directiva deve determinar até que ponto os dados pessoais podem ser recolhidos, armazenados e tratados em ligação com a oferta de serviços de telecomunicações;

14. Considerando que a recolha, armazenamento e tratamento de dados pessoais por parte de uma organização de telecomunicações se justifica apenas para efeitos da oferta do serviço previsto, nao podendo aqueles dados ser objecto de utilização para qualquer outro fim sem uma autorização legal específica ou o prévio consentimento escrito do assinante; que a recolha, o armazenamento e o tratamento de dados pessoais referidos nao podem, nomeadamente, ser utilizados de modo a dar à referida organização de telecomunicações qualquer vantagem concorrencial indevida sobre outros prestadores de serviços;

15. Considerando que a presente directiva deve pôr em prática, no sector das telecomunicações, os princípios gerais dos direitos dos assinantes relativos à inspecção dos dados pessoais a seu respeito armazenados e à rectificação ou apagamento desses dados, se necessário, bem como à prevenção da divulgação nao autorizada dos seus dados pessoais;

16. Considerando que a presente directiva deve prever a harmonização da regulamentação nos Estados-membros relativa à protecção da vida privada no campo dos registos discriminados de chamadas;

17. Considerando que, no que respeita à identificação da linha chamadora, é necessário proteger quer o direito da parte que efectua a chamada manter o anonimato, quer a vida privada da parte chamada em relação a chamadas nao identificadas;

18. Considerando que devem ser previstas medidas de protecção dos utilizadores de serviços de telecompra e videotex contra a utilização nao autorizada dos seus dados pessoais, bem como dos assinantes em geral contra a intrusão na sua vida privada por meio de chamadas nao solicitadas;

19. Considerando que deve garantir-se que a introdução de características técnicas nos equipamentos de telecomunicações para efeitos de protecção dos dados seja harmonizada a fim de ser compatível com a realização do mercado interno de 1992;

20. Considerando que a execução da presente directiva no que respeita a países terceiros deve ter em conta o nível de protecção de dados pessoais e da vida privada nesses países, sendo esta questão abordada na directiva do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais;

21. Considerando que em todas as matérias relativas à protecção de dados e da vida privada no contexto das redes públicas de telecomunicações digitais que não sejam abrangidas pelo disposto na presente directiva se aplicará a referida directiva do Conselho;

22. Considerando que a presente directiva nao aborda questões de protecção de dados pessoais e protecção da vida privada relacionadas com a segurança nacional;

23. **Considerando que é útil, na preparação de medidas destinadas à execução ou alteração da presente directiva, recorrer à experiência do grupo composto por representantes das autoridades que controlam a protecção de dados pessoais,** criado nos termos do artigo 27º da Directiva ....do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais;

24. **Considerando que tais medidas devem ser preparadas com a assistência do comité formado por representantes dos Estados-membros,** criado nos termos do artigo 30º da Directiva ...(CEE) do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais,

ADOPTOU A PRESENTE DIRECTIVA:

Artigo 1º

1. A presente directiva prevê a harmonização das disposições necessárias para garantir o mesmo nível de protecção da vida privada na Comunidade e para proporcionar a livre circulação de equipamentos e serviços de telecomunicações nos Estados-membros e entre estes.

2. Os Estados-membros adoptarão nos termos da presente directiva as disposições específicas necessárias para garantir a protecção de dados pessoais e da vida privada no sector das telecomunicações.

Artigo 2º

Sem prejuízo das disposições gerais da Directiva ....(CEE) do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais, a presente directiva aplica-se especificamente à recolha, armazenamento e tratamento de dados pessoais por parte de organizações de telecomunicações em ligação com a oferta de serviços públicos de telecomunicações nas redes públicas digitais de telecomunicações na Comunidade, nomeadamente através da Rede Digital de Serviços Integrados (RDSI) e das redes públicas móveis digitais.

2. Caso um Estado-membro nao tenha aínda criado a Rede Digital de Serviços Integrados (RDSI) ou redes públicas móveis digitais, o disposto na presente directiva é aplicável na medida em que também se aplique a serviços baseados em redes analógicas.

Artigo 3º

Para efeitos da presente directiva entende-se por :

1. "dados pessoais" quaisquer informações relacionadas com uma pessoa identificada ou identificável.

2. "organização de telecomunicações" um organismo público ou privado ao qual um Estado-membro concede direitos especiais ou exclusivos para a oferta de uma rede pública de telecomunicações e, quando for o caso, de serviços públicos de telecomunicações.

3. " rede pública de telecomunicações" a infra-estrutura pública de telecomunicações que permite a passagem de sinais entre pontos terminais da rede definidos por fios, microondas, meios ópticos ou outros meios electromagnéticos.

4. " serviço público de telecomunicações" um serviço de telecomunicações cuja oferta foi confiada especificamente pelos Estados-membros, entre outros, a uma ou mais organizações de telecomunicações.

Artigo 4º

1. A recolha, armazenamento e tratamento de dados pessoais por parte de uma organização de telecomunicações justifica-se apenas para efeitos de telecomunicações, nomeadamente para o estabelecimento de ligações para a transmissão de voz, dados ou imagens, produção de facturas, elaboração de listas de assinantes e outros fins

operacionais legítimos, como seja eliminação de avarias, prevenção do uso indevido do equipamento da organização de telecomunicações ou registo das chamadas de entrada, nos termos do número 1 do artigo 13º.

2. A organização de telecomunicações nao utilizará aqueles dados para estabelecer perfis electrónicos dos assinantes ou classificações de assinantes individuais por categoria.

Artigo 5º

1. Podem ser coligidos e armazenados dados pessoais do assinante na medida do necessário para concluir, alterar ou pôr termo ao contrato com a organização de telecomunicações. Após o termo do contrato os dados devem ser apagados, a menos que e enquanto sejam necessários para efeitos de queixas, cobranças ou cumprimento de outras obrigações impostas pela legislação do Estado-membro em conformidade com a legislação comunitária.

2. O conteúdo das informações transmitidas não pode ser armazenado pela organização de telecomunicações após o final da transmissão, a nao ser que tal decorra de obrigações impostas pela legislação do Estado-membro em conformidade com a legislação comunitária.

Artigo 6º

1. O assinante tem direito a:

- obter, com uma periodicidade razoável e sem demora ou despesa excessiva, a confirmação da existência ou não existência de armazenamento de dados pessoais a seu respeito, bem como a que lhe sejam comunicados tais dados sob forma inteligível;

- obter, se for caso disso, a rectificação ou o apagamento daqueles dados, quando tenham sido tratados de modo contrário às disposições impostas pelo Estado- membro em conformidade com o direito comunitário.

Artigo 7º

1. Em princípio, todos os dados pessoais tratados em ligação com redes e serviços de telecomunicações devem ser mantidos confidenciais.

2. Os dados pessoais nao podem ser divulgados para fora dos serviços ou da rede da organização de telecomunicações sem permissão legal especifica ou prévio consentimento do assinante. Só se considera que um assinante deu o referido consentimento quando este foi dado através de uma resposta especifica a um pedido feito pela organização de telecomunicações. Sem o prévio consentimento do assinante aqueles dados pessoais nao devem ser divulgados a pessoas que, dentro da organização de telecomunicações, nao se ocupam dos serviços prestados em questão.

3. A organização de telecomunicações nao pode fazer depender daquele consentimento a prestação do seu serviço.

Artigo 8º

1. A organizaçao de telecomunicações deve assegurar uma protecção adequada, ao nível do estado da técnica, dos dados pessoais contra acesso e utilização nao autorizados.

2. Em caso de risco especial de violação da segurança da rede, por exemplo, no domínio da radiotelefonia móvel, a organização de telecomunicações deve informar os assinantes acerca daquele risco e oferecer-lhes um serviço de cifragem de extremo a extremo.

Artigo 9º

1. Podem ser armazenados e tratados dados de facturação que contenham o número de telefone ou a identificação do posto do assinante, o endereço do assinante e o tipo de posto, o número total de unidades a cobrar para o período de contagem, o número do telefone chamado, o tipo e a duração das chamadas feitas e/ou o volume de dados transmitidos, bem como outras informações necessárias para a facturação, como pagamentos avançados, pagamentos em prestações, desligamento e notas.

2. O referido armazenamento geral de dados de facturação é permissível até final do período legal durante o qual a factura pode ser contestada.

Artigo 10º

1. Podem ser recolhidos, armazenados e tratados dados referentes ao tráfego que contenham os dados pessoais necessários para o estabelecimento de chamadas ou para facturação ou outros fins operacionais, como o número do telefone do assinante chamador e chamado, a hora de início e fim de cada chamada e o serviço de telecomunicações utilizado pelo assinante, na medida em que tal seja necessário à prestação do serviço de telecomunicações pretendido.

2. Os dados referentes a tráfego armazenados nos centros de comutação da organização de telecomunicações devem ser apagados após o fim da chamada, a menos que os dados sejam tornados anónimos ou necessários para facturação ou outros fins legitimos nos termos do artigo 4º.

Artigo 11º

A pedido do assinante poderão ser produzidas informações discriminadas de chamadas contendo, entre outros elementos, os números dos telefones dos assinantes chamados sem os últimos quatro digítos.

Artigo 12º

1. No que respeita às comunicações entre assinantes ligados a centrais digitais, o assinante chamador deve ter a possibilidade de eliminar, através de meio técnico simples, a identificação do seu número de telefone no visor do equipamento terminal do assinante chamado ou o registo daquele número num dispositivo de armazenamento daquele terminal, de modo casuístico.

   A transmissão do número do telefone pode também ser permanentemente eliminada pela organização de telecomunicações a pedido do assinante chamador.

2. O assinante chamado pode pedir a eliminaçao permanente da identificação de todas as chamadas de entrada; deve também poder desligar o visor do seu equipamento terminal ou suprimir o registo no dispositivo de armazenamento do terminal, a fim de evitar a identificação das chamadas de entrada, de modo casuístico.

   O assinante chamado deve poder limitar a aceitação das chamadas de entrada às que identificam o número do assinante chamador.

3. No que respeita a comunicações entre um assinante ligado a uma central analógica e assinantes ligados a centrais digitais, aquele assinante deve ser informado sobre a identificação do seu número de telefone e ter a possibilidade de obter, a pedido, a eliminação permanente daquela identificação. O assinante deve ter também a possibilidade de eliminar a identificação de modo casuístitico.

Artigo 13º

1. Durante um período de tempo limitado, a organização de telecomunicações pode anular a eliminação da identificação da linha chamadora

   a) a pedido de um assinante que pretenda identificar chamadas maliciosas. Nestes casos, os dados que contêm a identificação do assinante chamador serao armazenados pela organização de telecomunicações e, a pedido, colocados à disposição da autoridade pública do Estado-membro em causa encarregada da prevenção ou averiguação de delitos;

   b) por mandato judicial específico, a fim de prevenir ou proceder à averiguação de delitos criminais graves.

2. Uma função de anulação permanente deve, a pedido, ser posta à disposição

   a) de organizações reconhecidas por um Estado-membro que respondam e se encarreguem de chamadas de emergência e

   b) de organizações de bombeiros geridas ou reconhecidas por um Estado-membro.

3. As organizações de telecomunicações tomarão as medidas necessárias para garantir que a função de anulação fique operacional à escala nacional e comunitária.

Artigo 14º

1. O reencaminhamento de chamadas do assinante chamado para terceiros só pode ser efectuado se estes derem o seu acordo; os terceiros podem limitar o reencaminhamento às chamadas que identificam o número do assinante chamador e devem ser informados, por meio de um sinal específico da mensagem, de que a chamada foi reencaminhada.

2. O assinante chamador deve ser informado automaticamente durante o estabelecimento da ligação de que a chamada está a ser reencaminhada para terceiros.

Artigo 15º

1. No caso de o conteúdo das chamadas telefónicas ficar acessível a terceiros através de dispositivos técnicos, como altifalantes ou outros equipamentos incorporados no aparelho, ou armazenado em banda para uso próprio ou para uso de terceiros, devem prever-se medidas destinadas a informar os interessados, através de processo adequado, da referida difusão ou armazenamento antes que tal difusão ou armazenamento tenha início e enquanto durar.

2. O nº 1 nao se aplica nos casos abrangidos pelo número 1 do artigo 13º.

Artigo 16º

1. A organizaçao de telecomunicações deve garantir que o número de telefone assim como outros dados pessoais do assinante, nomeadamente respeitantes à quantidade e natureza das suas encomendas aquando da utilização de um serviço de telecompra ou respeitantes a informações pedidas através de um serviço videotex, sao armazenados somente na medida do estritamente necessário para oferecer o serviço e utilizados pelo prestador de serviços apenas para fins autorizados por aquele assinante.

2. Sem prejuízo do disposto no artigo 20º, o prestador de serviços nao pode estabelecer perfis electrónicos dos assinantes ou classificações de assinantes individuais por categoria sem o seu prévio consentimento.

Artigo 17º

1. Os assinantes que recebem chamadas nao solicitadas para efeitos de publicidade ou de oferta de bens e serviços têm o direito de notificar à organização de telecomunicações que lhes faz chegar aquelas mensagens que não desejam receber as referidas chamadas.

2. A organização de telecomunicações deve tomar as medidas necessárias para pôr fim à transmissão de tais mensagens para os assinantes em questão. A organização de telecomunicações deve ainda manter uma lista das notificações sob forma especificada pela autoridade tutelar e colocá-la à disposição desta, a fim de evitar, de futuro, aquelas chamadas.

Artigo 18º

1. Na execução do disposto na presente directiva, os Estados-membros devem garantir, sem prejuízo do disposto nos nºs 2 e 3 do presente artigo, a nao imposição de quaisquer requisitos obrigatórios de características técnicas específicas a equipamentos terminais ou outros de telecomunicações que possam impedir a colocação no mercado de equipamentos e a livre circulação de tais equipamentos nos Estados-membros e entre estes.

2. Nos casos em que a execução das disposições só possa ser feita através da exigência de características técnicas específicas, os Estados-membros informarão a Comissão nos termos dos processos previstos na Directiva 83/189/CEE do Conselho(10) que estabelece um procedimento de informação no domínio das normas e regulamentações técnicas.

3. Sempre que necessário, a Comissão assegurará a elaboração de normas europeias comuns na realização de características técnicas específicas, nos termos da Directiva ...(CEE) do Conselho [relativa à aproximação das legislações dos Estados-membros respeitantes a equipamentos terminais de telecomunicações,](11), incluindo o reconhecimento mútuo da sua conformidade e da Decisão 87/95/CEE do Conselho de 22 de Dezembro de 1986 relativa à normalização no domínio das tecnologias da informação e das telecomunicações(12).

Artigo 19º

1. As disposições da presente directiva relativas ao serviço telefónico sao aplicáveis a outros serviços públicos de telecomunicações digitais na medida em que tais serviços apresentem riscos similares para a vida privada do utilizador.

2. As medidas necessárias para execução do nº 1 serão adoptadas pela Comissão após consulta do grupo referido no artigo 22º e nos termos do procedimento estabelecido no artigo 23º.

---

(10) JO nº L 109 de 26.4.1983, p. 8.

(11) JO nº C

(12) JO nº L 36 de 7.2.1987, p. 31.

Artigo 20º

Na medida em que a plena realização dos objectivos da presente directiva exige a aplicação das suas disposiçoes a prestadores de serviços que nao sejam organizações de telecomunicações, a Comissão pode adoptar as medidas necessárias para a aplicação da presente directiva àqueles prestadores de serviços após consulta do grupo referido no artigo 22º e nos termos do procedimento estabelecido no artigo 23º.

Artigo 21º

Os pormenores relativos à aplicação da presente directiva e as alterações necessárias para adaptar a presente directiva aos novos avanços técnicos sao determinados pela Comissão nos termos do procedimento estabelecido no artigo 23º.

Artigo 22º

1. O Grupo de protecção dos dados pessoais criado nos termos do artigo 27º da Directiva ... do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais desempenhará as atribuições previstas no artigo 28º daquela directiva igualmente em relação às medidas de protecção de dados que sao objecto da presente directiva.

2. O Grupo será constituído especificamente para os fins da presente directiva.

Artigo 23º

1. É aplicável o procedimento previsto no artigo 30º da Directiva ...(CEE) do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento dos dados pessoais.

2. O Comité criado no âmbito do referido procedimento será constituído especificamente para os fins da presente directiva.

Artigo 24º

1. Os Estados-membros porao em vigor as disposições legislativas, regulamentares e administrativas necessárias para darem cumprimento à presente directiva o mais tardar até 1 de Janeiro de 1993.

As disposições adoptadas nos termos do primeiro parágrafo referir-se-ão explicitamente à presente directiva.

2. Os Estados-membros comunicarão à Comissao o texto das disposições de direito interno que adoptarem no domínio abrangido pela presente directiva.

Artigo 25º

Os Estados-membros sao os destinatários da presente directiva.

Feito em Bruxelas, em

Pelo Conselho

FICHE FINANCIERE

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLICS, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES MOBILES PUBLICS.

1. Ligne budgétaire concernée

En 1990 : B 7700

En 1991 et exercices ultérieurs : B5-4010

2. Base légale

Article 100 A

3. Proposition de classification en dépense obligatoire /non obligatoire

non -obligatoire

4. Description et justification de l'action :

4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,

- permettre la circulation transfrontalière de données à caractère personnel dans la Communauté,

- permettre le bon fonctionnement du marché intérieur.

4.2. Réunions spécifiques du groupe de protection des données à caractère personnel (Art. 22) et du Comité consultatif (Art. 23), créés par la directive, représentant les Etats membres .

4.3. Un représentant de la Commission préside le groupe de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du groupe et du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. **Nature : réunions**

(frais de participation des membres des 2 Comités)

5.2. Calcul : - Groupe de protection des données : (cf. fiche financière de la directive générale)

- Comité consultatif :

24 membres (gouvernementaux) x 3 réunions x 2 jours x 390 ECU/jour = 56.160 ECU *

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echéancier des crédits d'engagement et de paiement

CE-CP

1993 : 56.160 ECU

1994 : 56.160 *

1995 : 56.160 *

1996 : 56.160 *

1997 : 56.160 *

6.2. Part du financement communautaire dans le coût total : 100 %

---

* estimation

7. Observations :

1. Le groupe de protection des données à caractère personnel (Art. 22):

Il est institué ce groupe à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tous les Etats membres, présidé par un représentant de la Commission.

Ce groupe établit son règlement intérieur. Le secrétariat du groupe est assuré par les services de la Commission.

Missions de ce groupe : voir Art. 22

2. Le Comité consultatif (Art . 23)

Il est institué un Comité consultatif composé des représentants des Etats Membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.

Recomendação de

DECISÃO DO CONSELHO

relativa à abertura de negociações com vista à adesão da Comunidade Europeia à Convenção do Conselho da Europa para a protecção dos indivíduos, relativamente ao tratamento automatizado de dados de carácter pessoal

Exposição dos motivos

1. A protecção dos indivíduos relativamente ao tratamento de dados pessoais constitui simultaneamente um direito do indivíduo e uma condição necessária para o desenvolvimento do comércio internacional.

2. O tratamento de dados de carácter pessoal é indispensável para a realização de intercâmbios internacionais de bens e de serviços e para uma colaboração mais estreita entre os países.

3. A Comissão apresentou ao Conselho uma proposta de directiva que visa assegurar, no conjunto da Comunidade, um nível de protecção elevado dos indivíduos relativamente ao tratamento dos dados de carácter pessoal. Seria conveniente que esta acção se fizesse acompanhar de iniciativas que visem garantir aos indivíduos um nível de protecção equivalente aquando do intercâmbio de dados entre a Comunidade e os países terceiros.

4. Em 1981, o Conselho da Europa elaborou uma Convenção sobre a protecção dos indivíduos relativamente ao tratamento automatizado dos dados de carácter pessoal. A finalidade desta Convenção é garantir no território de cada uma das partes, a todas as pessoas singulares, quaisquer que sejam as suas nacionalidades ou residências, o respeito dos seus direitos e das suas liberdades fundamentais e, nomeadamente, do seu direito à privacidade relativamente ao tratamento automatizado de dados de carácter pessoal a elas relativos. Esta Convenção prevê ainda que uma parte não pode, exclusivamente com a finalidade da protecção da vida privada, proibir ou submeter a uma autorização especial os intercâmbios transfronteiriços de dados de carácter pessoal destinados ao território de outra parte.

5. Na sua Recomendação de 29 de Julho de 1981, a Comissão convidou os Estados-membros da Comunidade a ratificar a Convenção do Conselho da Europa sobre a protecção dos indivíduos relativamente ao tratamento automatizado dos dados de carácter pessoal precisando que, se todos os Estados-membros não assinassem e ratificassem esta Convenção num prazo razoável, a Comissão se reservaria o direito de apresentar ao Conselho uma proposta para a adopção de um acto de base no Tratado CEE.

6. Por enquanto, nem todos os Estados-membros da Comunidade ratificaram esta Convenção(1). É desejável e necessário que a Comunidade adira à Convenção para assegurar a protecção e a circulação transfronteiriça dos dados de carácter pessoal com os países terceiros e para tornar mais interessante a Convenção para os países terceiros que pretendam efectuar um intercâmbio de dados, tão livre quanto possível, com a Comunidade.

---

(1) Relativamente aos Estados-membros da Comunidade, a Convenção (STE 106 de 28 de Janeiro de 1981) foi assinada pela Bélgica, Grécia, Irlanda, Itália, Países Baixos e Portugal; esta Convenção foi ratificada pela Dinamarca, França, República Federal da Alemanha, Luxemburgo, Espanha e Reino Unido.

7. Consequentemente, a Comissão recomenda ao Conselho que a autorize a negociar, com o Conselho da Europa e os Estados participantes na Convenção sobre a protecção dos indivíduos relativamente ao tratamento automatizado dos dados de carácter pessoal, um protocolo adicional que permita às Comunidades Europeias participar nesta Convenção, nos domínios da sua competência.

8. A Comissão conduzirá estas negociações, em consulta com os representantes dos Estados-membros, no quadro das directrizes anexas à presente comunicação ou das que lhe sejam eventualmente dirigidas pelo Conselho.

9. Os Estados-membros da Comunidade, membros do Conselho da Europa, apoiarão plenamente a acção da Comunidade ao longo das negociações para a adesão da Comunidade Europeia, assim que esta questão for evocada nos órgãos do Conselho da Europa.

Anexo: Directrizes para as negociações

ANEXO

DIRECTRIZES PARA AS NEGOCIAÇÕES

1. As negociações visam assegurar a conclusão de um protocolo adicional que permita à Comunidade tornar-se parte contratante da Convenção nos domínios da sua competência, no respeito dos princípios a seguir enumerados:

2. No seio do Comité Consultivo instituído pelo artigo 18º da Convenção, a Comunidade Europeia será representada, enquanto membro, pela Comissão das Comunidades Europeias.

   Após coordenação comunitária, cuja iniciativa é da responsabilidade da Comissão, o representante da Comunidade Europeia terá à sua disposição um número de votos correspondente à soma dos votos das delegações nacionais dos Estados-membros da Comunidade participantes na Convenção, para todas as questões relativas aos tratamentos de dados de carácter pessoal nos domínios da competência comunitária.

   Para as outras questões, cada delegação nacional terá direito a um voto.

3. A fim de permitir a entrada em vigor, num prazo razoável, do protocolo adicional que permitirá à Comunidade tornar-se parte contratante da Convenção, a Comissão proporá, com o apoio dos Estados-membros, que seja incluído no texto do protocolo uma disposição de "notificação negativa" (opting out procedure) para a adopção do protocolo adicional.

Proposta de

DECISÃO DO CONSELHO

NO DOMÍNIO DA

SEGURANÇA DA INFORMAÇÃO

Resumo

A informação, nas suas várias formas, contribui cada vez mais para a riqueza das pessoas, das empresas e das nações. O crescimento e as realizações de cerca de 2/3 da economia baseiam-se em actividades de produção ou de serviços fortemente dependentes das tecnologias da informação, das telecomunicações e da radiodifusão e, como tal, dependem de forma crítica da precisão, segurança e credibilidade da informação. Isto reveste-se de grande importancia e interesse para os indivíduos, o comércio, a indústria e as administrações públicas. Consequentemente, a protecção da informação em todos os seus aspectos, aqui denominada segurança da informação(1), tornou-se uma questão política central e uma importante preocupação em todo o mundo.

Nas últimas décadas ocorreram importantes mudanças, mas as que estão para vir podem ser ainda maiores. Supercomputadores de escritório, radiodifusão directa por satélite, rádio digital móvel, comunicações integradas em banda larga e outras aplicações novas das tecnologias estão em desenvolvimento e fornecerão os meios para comunicações de baixo custo, móveis e de alto nível de desempenho em todo o mundo, numa escala sem precedentes. O advento de comunicações globais eficientes veio sublinhar ainda mais a necessidade de proporcionar uma protecção "adequada" em níveis de disponibilidade dos serviços, integridade das mensagens e privacidade correspondentes ao nível previsto de ameaças administrativas ou técnicas.

O tema é de grande importância para o desenvolvimento socioeconómico da Comunidade Europeia e a realização do mercado interno em 1992. Uma abordagem coerente a nível europeu deveria criar simultaneamente um sentimento crescente de confiança em relação à utilização dos novos serviços das tecnologias da informação e telecomunicações e ajudar a evitar a formação de novas barreiras entre os Estados-membros ou entre estes e outros países. Há, pois, uma necessidade urgente de estudar os requisitos e opções com vista a uma acção a nível comunitário em estreita colaboração com os intervenientes no sector e os Estados-membros. Qualquer acção deve ter em conta a evolução comercial, jurídica e técnica, tanto a nível nacional como internacional. Como a segurança da informação abrange a protecção não só de pessoas e bens, mas também da própria sociedade, os Estados-membros consideram-na como uma questão no âmbito da soberania nacional.

Ao mesmo tempo, tanto para a Comunidade como para os seus Estados-membros, é vital que a segurança da informação não se torne uma restrição à promoção do desenvolvimento harmonioso na Comunidade e às relações com

(1) Segurança da informação (SI) diz respeito à protecção da informação armazenada, tratada ou transmitida sob forma electrónica contra ameaças acidentais ou deliberadas. Os serviços de informação electrónica necessitam de infra-estrutura de telecomunicações segura, terminais seguros (incluindo processadores e bases de dados) e procedimentos de utilização seguros.

outros países. Assim, o desenvolvimento de uma abordagem harmonizada da segurança da informação deve fazer parte integrante das políticas comunitárias relacionadas com o reforço das realizações socioeconómicas, a competitividade internacional e a realização do mercado interno da Comunidade Europeia.

> *A questão fundamental é fornecer uma segurança efectiva e prática da informação mantida sob forma electrónica para os utilizadores em geral, as administrações e o sector dos negócios sem comprometer os interesses do público em geral.*

Uma acção a nível comunitário deverá implicar esforços concertados para estabelecer as necessárias tecnologias, normas, procedimentos de verificação e certificação e (se necessário) regulamentações no âmbito da elaboração da política comunitária.

A intenção da Comissão é encorajar um debate com os intervenientes no sector na Comunidade sobre questões de segurança da informação e desenvolver um consenso sobre os passos adequados a considerar. Este debate poderá ser iniciado com base na declaração de princípios e linhas de acção identificados no Anexo desta nota. Neste debate, e dadas as responsabilidades dos Estados-membros neste domínio, é de crucial importância que a iniciativa comunitária se possa apoiar numa estreita colaboração com altos funcionários dos Estados-membros.

Deste modo, propõe-se que a Comissão seja assistida por um Comité de natureza consultiva, composto por representantes dos Estados-membros e presidido pelo representante da Comissão. O funcionamento deste comité deve reflectir as especificidades do domínio. Este comité denominar-se-ia Grupo de Altos Funcionários para a Segurança da Informação (SOG-IS). A sua missão e composição estão descritas nos números 37 a 39 da presente comunicação.

A questão mais importante da protecção de dados pessoais é tratada numa proposta de directiva apresentada em paralelo com a presente comunicação.

A. Os novos desafios e a importância social, económica, estratégica e política da segurança da informação.

1. A gestão e utilização da informação apoiada nas tecnologias da informação e nos serviços informáticos invade todas as esferas da vida económica social e política. Isto permitiu a integração de actividades através de um sistema global de comunicações que liga unidades de produção, estabelecimentos de investigação, bases de dados, centros informáticos, prestadores de serviços e ainda os centros de decisão política e económica.

2. Esta integração crescente de actividades separadas gera um valor acrescentado considerável em termos de poupança ou aumento de eficiência. Trata-se, pois, de um factor essencial da competitividade internacional. Contudo, ela faz também aumentar a necessidade de proteger os justos interesses dos indivíduos, do público em geral, do comércio, da indústria, dos operadores, dos prestadores de serviços e das administrações nacionais.

3. Para que o sector dos serviços cresça e sejam efectuados investimentos em equipamentos electrónicos, telecomunicações, radiodifusão, computadores e equipamentos terminais e numa vasta gama de aplicações telemáticas, há que oferecer um ambiente europeu seguro para a informação electrónica. Uma aceitação e aprovação generalizada por parte de todos os interessados é importante para salvaguardar interesses legítimos e prevenir abusos e utilizações indevidas da informação. Isto deve ser realizado de modo simultaneamente eficiente e adequado a utilizadores submetidos a diferentes sistemas jurídicos. Além do mais, os sistemas de segurança da informação devem proteger a privacidade, a propriedade intelectual, a concorrência leal, a segurança nacional e outros interesses.

4. Com a introdução dos microcomputadores, a utilização das tecnologias da informação, das telecomunicações e da radiodifusão ultrapassou o domínio profissional e tornou-se uma "actividade de consumidor" com os correspondentes "serviços de consumidor". A par desta mudança quantitativa, deu-se uma mudança qualitativa muito significativa: as telecomunicações permitem actualmente o interfuncionamento e a comunicação numa escala global.

5. Nas últimas décadas ocorreram grandes mudanças, mas as que se avizinham podem ser ainda maiores. Supercomputadores de escritório, radiodifusão directa por satélite, rádio digital móvel, comunicações integradas em banda larga e outras novas aplicações das tecnologias estão em desenvolvimento e fornecerão os meios para comunicações de baixo custo, móveis e de alto nível de desempenho em todo o mundo, numa escala sem precedentes.

6. O advento de comunicações globais suficientes representa um desafio qualitativa e quantitativamente novo para a necessidade de proporcionar "protecção" adequada em níveis de disponibilidade dos serviços, integridade das mensagens e privacidade em correspondência com o nível previsto das ameaças administrativas ou técnicas.

7. O desejo crescente da indústria, do governo e da sociedade em geral utilizarem os serviços da informação fez com que estes se tornassem parte integrante do modo de vida quotidiano. As funções de comando, comunicação e controlo em geral, o controlo de processos na produção, nos transportes, nos serviços financeiros, nos sistemas burótícos, etc., exigem todos eles, níveis de disponibilidade e robustez operacional que não foram inteiramente previstos na concepção inicial do serviço ou do componente.

8. Serão definidas e realizadas novas aplicações que não poderão ser postas em funcionamento no quadro das arquitecturas actuais. Pode vir a ser necessária uma redefinição fundamental de arquitecturas e normas de desempenho (incluindo a necessidade de garantir conformidade) relacionadas com os serviços e os componentes subjacentes.

9. Terão que ser criadas novas disciplinas e organizações/ocupações e apoio para se atingirem estes níveis mais elevados de exigências funcionais. No entanto, as principais necessidades serão determinadas por mudanças culturais e não técnicas. A exploração global dos serviços da informação apoiados por redes globais de telecomunicações mudará a percepção das relações organizativas/humanas na sociedade.

10. A comunicação far-se-á cada vez mais através de intermediários, como nos diversos níveis de serviços de valor acrescentado suportados pelas TI, ou directamente, após a aprovação, por intermediários, do contacto. Nestas situações, será necessários definir explicitamente a confiança no contexto de relações organizativas, autoridades/privilégios e muitos "controlos de qualidade" dos serviços/produtos. Deve haver o cuidado de, numa tal sociedade, os direitos dos indivíduos e das organizações se reflectirem plenamente na legislação e nos controlos regulamentares. Paralelamente, as tecnologias devem ser concebidas e realizadas de modo a satisfazerem as exigências de segurança.

B. Necessidade de uma acção a nível comunitário em colaboração com os Estados-membros

11. Estando em jogo a protecção da propriedade, dos indivíduos e até da sociedade, é óbvio que a segurança da informação é uma área de grande responsabilidade para os Estados-membros. Tanto para a defesa como para o normal funcionamento das suas instituições, cada Estado-membro está directamente envolvido na segurança. Estas preocupações nacionais dos governos conduziram, historicamente, a uma competência sólida e durável no domínio da segurança da informação e do exercício de um controlo das suas tecnologias e técnicas, a fim de evitar a divulgação de aspectos melindrosos. Ainda que cada utilizador deva ser responsável pela escolha da sua própria segurança, as suas opções assentam essencialmente em garantias que, em última análise, são exigidas pelas autoridades públicas através, por exemplo, dos limites legais que fixam.

12. As políticas e os programas da CEE para o desenvolvimento das indústrias da informação e telecomunicações e para a realização do mercado interno podem deparar com sérios obstáculos, a menos que seja adoptada uma política activa de criação, desenvolvimento e promoção de normas de segurança para os serviços da informação. Para a Comunidade é vital que a segurança da informação não se torne um obstáculo à promoção de um desenvolvimento harmonioso na Comunidade e às relações com outros países. Assim, o desenvolvimento de uma abordagem harmonizada da segurança da informação deve fazer parte integrante das políticas comunitárias relacionadas com o reforço das realizações socioeconómicas e da competitividade internacional da indústria europeia e com a realização do mercado interno.

13. Mais precisamente, deve implicar esforços concertados para o estabelecimento das necessárias normas, procedimentos de verificação e certificação e desenvolvimentos e regulamentações (quando necessárias) tecnológicos no quadro da elaboração da política comunitária. Dada a natureza altamente técnica das questões subjacentes, a concertação de esforços implica a colaboração dos intervenientes na fase pré-competitiva de I&D.

14. A adopção de "normas abertas" por governos (GOSIP nos EUA e no Reino Unido), pela defesa ocidental (OTAN/NOSI), pela indústria de informática e telecomunicações e pelos operadores de rede (normas OSI da ISO) conduziu a um maior realce das questões de segurança em sistemas, arquitecturas, normas, protocolos de comunicações e técnicas de componentes no domínio da informação.

15. Apenas cerca de 2% dos serviços que estarão disponíveis na Comunidade no ano 2000 existem já neste momento. Nessa altura, os serviços poderão, em geral, responder às necessidades dos utilizadores e oferecer uma gama de características integradas que combinam voz, dados e imagens de forma flexível. A resposta às exigências dos utilizadores quanto à segurança da informação, como protecção de dados, privacidade, autenticação, autorização, facturação, etc., será, correspondentemente, muito mais difícil de garantir. É por esta razão que a segurança da informação e as características técnicas associadas, como a integridade, devem ser sistematicamente desenvolvidas e estudadas. As autoridades dos EUA estão a financiar programas sobre sistemas informáticos fiáveis, arquitecturas de sistemas abertos, protocolos e técnicas que acelerarão a utilização de soluções de segurança de fabricante na comunidade internacional dos utilizadores. Para os Estados-membros, ser parceiro em pé de igualdade na abordagem da normalização neste domínio deve constituir uma preocupação primordial. Ir atrás de uma normalização *de facto* trará o risco da criação de novas dependências tecnológicas que poderão dificultar seriamente a competitividade internacional das economias da Comunidade. Isto implica que os correspondentes esforços na Comunidade sejam um pré-requisito para uma interacção construtiva com países fora da Comunidade, principalmente os EUA.

16. Em resumo, devido às respectivas responsabilidades, tanto a Comunidade como os seus Estados-membros têm grande interesse nas seguintes questões essenciais :

- Como serão definidas e publicadas especificações e normas eficazes em matéria de segurança da informação ?
- Como será realizada a avaliação e certificação formal de conformidade de produtos e sistemas com as normas de segurança (tanto no plano funcional como no do fornecimento de garantia) ?
- Como serão realizados, fornecidos e utilizados os produtos e sistemas de segurança ?

17. A segurança da informação é um exemplo típico de uma política em que o princípio de *subsidiaridade* pode ser aplicado, dada a complexidade inerente ao tema, a presença de numerosos intervenientes e a necessidade de empregar uma grande variedade de instrumentos. É essencial um plano de acção que mostre o que deve ser feito, por quem e como. Por um lado, os Estados-membros têm que fazer face a estas questões; por outro, a Comunidade está fortemente interessada em chegar a uma solução que garanta a compatibilidade entre, por um lado, a realização do mercado interno e da Europa dos cidadãos, a execução de uma política de telecomunicações e a competitividade das indústrias e serviços comunitários da electrónica e dos serviços da informação electrónica e, por outro, a resposta às exigências básicas dos indivíduos e das empresas em matéria de segurança da informação. Assim, e para concentração de esforços, propõem-se abaixo vários tipos de acções e uma estrurura processual como ponto de partida para novos estudos em profundidade que conduzam às medidas a tomar nos níveis adequados.

Proposta de

DECISÃO DO CONSELHO

NO DOMÍNIO DA

SEGURANÇA DA INFORMAÇÃO

O CONSELHO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Económica Europeia e, nomeadamente, o seu artigo 235º,

Tendo em conta a proposta da Comissão,(1)

Tendo em conta o parecer do Parlamento Europeu,(2)

Tendo em conta o parecer do Comité Económico e Social,(3)

Considerando que a Comunidade tem como missão, através do estabelecimento de um mercado comum e da aproximação progressiva das políticas económicas dos Estados-membros, promover um desenvolvimento harmonioso das actividades económicas no conjunto da Comunidade, uma expansão contínua e equilibrada, uma estabilidade acrescida, uma elevação acelerada do nível de vida e relações mais estreitas entre os Estados-membros;

Considerando que a informação armazenada, tratada e transmitida electronicamente desempenha um papel cada vez mais importante nas actividades sociais e económicas;

Considerando que o advento de comunicações globais eficientes e a utilização em todos os domínios do tratamento electrónico da informação colocam em destaque a necessidade de uma protecção adequada;

---

(1) JO nº C ...

(2) JO nº C ...

(3) JO nº C ...

Considerando que o Parlamento Europeu sublinhou repetidamente a importância da segurança da informação nos seus debates e decisões;

Considerando que o Comité Económico e Social fez notar a necessidade de abordar questões relativas à segurança da inforprmação nas acções da Comunidade, nomeadamente tendo em vista o impacto da realização do mercado interno;

Considerando que é necessário desenvolver uma estratégia global de segurança da informação para garantir a segurança dos utilizadores a nível comunitário e evitar a criação de novos obstáculos técnicos à comunicação;

Considerando que a complexidade inerente às questões de segurança da informação exige a aplicação do conceito de subsidiaridade, a participação de diversos intervenientes no sector e o recurso concertado a diversas políticas;

Considerando que acções a nível nacional, internacional e comunitário porporcionam uma boa base;

Considerando que existe uma relação estreita com as políticas de telecomunicações, normalização, mercado da informaçção e ID&T e com os trabalhos já empreendidos nestes domínios pela Comunidade Europeia;

Considerando que é adequado garantir a concertação de esforços baseados em trabalhos existentes nacionais e internacionais e através da promoção da cooperação dos principais intervenientes em causa; que, consequentemente, é adequado prosseguir no quadro de um plano de acção coerente,

Considerando que a responsabilidade dos Estados-membros neste domínio implica uma abordagem concertada baseada numa estreita colaboraçao entre altos funcionários dos Estados-membros.

ADOPTOU A PRESENTE DECISÃO :

Artigo 1o

1. É adoptado um plano de acçao no domínio da segurança da informaçao (INFOSEC) por um periodo de 24 meses a partir de ( ).

2. O plano de acção destina-se a desenvolver uma estratégia global que proporcione aos utilizadores de informação armazenada, tratada ou transmitida electronicamente uma protecção da informação e dos sistemas de informação contra ameaças acidentais ou deliberadas.

3. A acção terá em conta e apoiará as actividades de normalização em curso a nivel europeu e mundial neste domínio.

Artigo 2o

O plano de acções referido no artigo 1º e cujos pormenores figuram em anexo compreeende as seguintes linhas de acção :

I. desenvolvimento de um quadro estratégico para a segurança da informação
II. exigências da segurança da informação
III. soluções para necessidades imediatas e temporárias
IV. especificações, normalização e verificação da segurança da informação
V. desenvolvimentos tecnológicos e operacionais no campo da segurança da informação
VI. oferta de segurança da informação.

Artigo 3o

O plano de acção é executado pela Comissão em colaboração com as organizações e empresas interessadas e em estreita associação com os Estados-membros.

Artigo 4o

O orçamento atribuído anualmente a esta acçao é determinado tendo em conta os procedimentos orçamentais.

Artigo 5o

A Comissão transmitirá ao Parlamento e ao Conselho um relatório sobre os resultados da acção num prazo de três meses após o seu termo.

Artigo 6o

Para execução do plano de acção, a Comissão consultará, na medida do necessário, um Grupo de Altos Funcionários para a Segurança da Informação (SOG-IS). Este grupo é constituído por dois representantes de cada Estado-membro e da Comissão. É presidido por um representante da Comissão.

Os membros do grupo podem ser apoiados por peritos ou consultores dependendo da natureza dos assuntos considerados.

As deliberações do grupo são confidenciais. O grupo adoptará o seu regulamento interno. O secretariado será garantido pela Commissao.

Feito em Bruxelas, em

Pelo Conselho

ANEXO

Resumo das Linhas de Acção

1. Linha de Acção I - Desenvolvimento de um Quadro Estratégico para a Segurança da Informação

1.1. Tema

1. A segurança da informação é reconhecida como uma qualidade necessária em expansão na sociedade moderna. Os serviços de informação electronica necessitam de uma infra-estrutura segura de telecomunicações, terminais seguros (incluindo processadores e bases de dados) e condições de utilização seguras. É necessário estabelecer uma estratégia global que tenha em conta todos os aspectos da segurança da informação, evitando uma abordagem fragmentada. Qualquer estratégia para a segurança da informação tratada sob forma electrónica deve reflectir a vontade de qualquer sociedade funcionar de forma eficaz, ao mesmo tempo que se protege num mundo em rápida mutação.

1.2 Objectivo

2. Deve ser criado um quadro estratégico que concilie os objectivos sociais, económicos e políticos com as opções técnicas, funcionais e legislativas. O equilíbrio delicado entre diferentes preocupações, objectivos e restrições deve ser achado pelos intervenientes no sector num trabalho conjunto de desenvolvimento de uma percepção comum e uma estratégia acordada. Tais são os pré-requisitos para a conciliação de interesses e necessidades tanto na elaboração de políticas como nos desenvolvimentos industriais.

1.3 Situação e tendências

3. A situação caracteriza-se por uma consciência crescente da necessidade de actuação. Contudo, na ausência de uma iniciativa de concertação de esforços, é muito provável que esforços dispersos em vários sectores venham a criar uma situação *de facto* com contradições, conduzindo ao aumento progressivo de importantes problemas jurídicos, sociais e económicos.

1.4 Necessidades, opções e prioridades

4. Um quadro assim partilhado exigirá a abordagem e tratamento da análise e gestão de riscos no que toca às vulnerabilidades da informação e dos serviços associados, ao alinhamento de legislações e regulamentações relacionadas com abusos e utilizações indevidas de computadores/telecomunicações, às infra-estruturas administrativas, incluindo as políticas de segurança e o modo como elas podem ser executadas de modo eficiente nas diferentes indústrias/disciplinas e às preocupações sociais e de privacidade (por exemplo, a aplicação de sistemas de identificação, autenticação e eventualmente autorização num ambiente democrático).

5. Deve ser fornecida uma orientação clara para o desenvolvimento de arquitecturas físicas e lógicas destinadas a serviços seguros de informação distribuída, normas, linhas de orientação e definições para produtos e serviços de segurança garantidos, experiências-piloto e protótipos para o estabelecimento da viabilidade de diferentes estruturas administrativas, arquitecturas e normas relacionadas com as necessidades de sectores específicos.

6. Deve ser promovida uma tomada de consciência em relação à segurança que influencie a atitude dos utilizadores, para que aumente o cuidado relativo à segurança nos sistemas das TI e telecomunicações.

2. Linha de Acção II - Exigências da Segurança da Informação

2.1 Tema

7. A segurança da informação é o pré-resquisito ligado à protecção de privacidade, propriedade intelectual, confidencialidade comercial e segurança nacional. Isto conduz inevitavelmente a um equilíbrio difícil e, por vezes, a escolhas entre um compromisso de comércio livre e um compromisso de garantia da privacidade e da propriedade intelectual. Estas escolhas e compromissos devem basear-se na plena apreciação das exigências e do impacto das possíveis opções para a segurança da informação destinadas a satisfazê-las.

8. As exigências dos utilizadores implicam funcionalidades de segurança da informação interdependentes com aspectos tecnológicos, operacionais e regulamentares. Deste modo, um estudo sistemático das exigências da segurança da informação faz parte integrante do desenvolvimento de medidas adequadas e efectivas.

2.2 Objectivo

9. Estabelecimento da natureza e características das exigências dos utilizadores e sua relação com as medidas de segurança da informação.

2.3 Situação e Tendências

10. Até hoje não foram empreendidos esforços destinados a identificar as exigências em rápida evolução e mutação dos principais intervenientes na segurança da informação. Os Estados-membros da CE identificaram as exigências de harmonização das actividades nacionais (nomeadamente os "critérios de segurança para as TI"). Revestem-se de grande importância critérios uniformes de avaliação e regras de reconhecimento mútuo de resultados/certificados de avaliação.

2.4 Necessidades, Opções e Prioridades

11. Como base para um tratamento coerente e transparente das necessidades justificadas dos intervenientes no sector, considera-se ser necessário desenvolver uma classificação acordada das exigências dos utilizadores e sua relação com a oferta de segurança da informação.

12. Considera-se também importante identificar necessidades no domínio da legislação, regulamentações e códigos de conduta à luz duma avaliação das tendências das características e tecnologias dos serviços, identificar estratégias alternativas para a consecução dos objectivos por meio de disposições administrativas, de serviço, operacionais e técnicas e avaliar a eficiência, a facilidade de utilização e os custos de opções e estratégias alternativas em segurança da informação para utilizadores, prestadores de serviços e operadores.

3. Linha de Acção III - Soluções para Necessidades Imediatas e Temporárias

3.1 Tema

13. Actualmente é possível proteger adequadamente os computadores contra o acesso não autorizado a partir do exterior através de "isolamento", ou seja, através da aplicação de medidas organizativas e físicas convencionais. O mesmo se aplica às comunicações electrónicas num grupo fechado de utilizadores funcionando numa rede dedicada. A situação é muito diferente caso a informação seja partilhada entre grupos de utilizadores ou transferida através de uma rede pública ou de acesso generalizado. Tanto a tecnologia, os terminais e os serviços como as normas e procedimentos associados são, em geral, incapazes de oferecer um nível comparável de segurança da informação nestes casos.

3.2 Objectivo

14. O objectivo deve ser o de fornecer, a curto prazo, soluções que possam responder às necessidades mais urgentes dos utilizadores. Devem ser concebidas de modo aberto às futuras necessidades e soluões.

3.3. Situação e tendências

15. Alguns grupos de utilizadores desenvolveram técnicas e procedimentos para uso próprio que respondem, nomeadamente, às necessidades de autenticaçção, integridade e não repúdio. São utilizados, em geral, cartões magnéticos ou cartões inteligentes. Por vezes utilizam-se técnicas mais ou menos sofisticadas de criptografia. Muitas vezes isto implica a definição de "autoridades" específicas de grupos de utilizadores. Contudo, é difícil generalizar estas técnicas e métodos por forma a responderem às necessidades de um ambiente aberto.

16. A ISO está a trabalhar na segurança da informação OSI (ISO DIS 7498-2), tal como o CCITT no contexto do X400. É também possível inserir segmentos de segurança da informação nas mensagens. Autenticação, integridade e não repúdio estão a ser tratados como parte das mensagens (EDIFACT) e do X400 MHS.

17. Actualmente, o quadro jurídico da EDI está ainda em fase de concepão. A Câmara de Comércio Internacional publicou regras uniformes de conduta para a transferência de dados comerciais através de redes de telecomunicações.

18. Vários países (por exemplo, RFA, França, Reino Unido e EUA) desenvolveram ou estão a desenvolver os critérios para avaliação da fiabilidade de produtos e sistemas das TI e telecomunicações e os procedimentos correspondentes para a realização das avaliações. Estes critérios foram coordenados com os fabricantes nacionais e conduzirão a um número crescente de produtos e sistemas fiáveis, a começar em produtos simples. A criação de organizações nacionais que efectuem as avaliações e emitam os certificados constituirá um apoio a esta linha de esforços.

19. A oferta de confidencialidade é considerada pela maioria dos utilizadores como menos importante no imediato. Contudo, no futuro esta situação irá provavelmente mudar, na medida em que se generalizem serviços de comunicações avançadas, nomeadamente os serviços móveis.

3.4 Necessidades, opções e prioridades

20. É essencial desenvolver o mais rapidamente possível os procedimentos, normas, produtos e instrumentos adequados para garantir a segurança da informação nas redes públicas de comunicações. Deve ser concedida prioridade elevada a autenticação, integridade e não repúdio. Devem realizar-se projectos-piloto destinados a estabelecer a validade das soluções propostas. O programa TEDIS procura soluções para necessidades prioritárias em EDI no âmbito mais geral do presente plano de acção.

4. Linha de Acção IV - Especificações, Normalização e Verificação da Segurança da Informação

4.1 Tema

21. As exigências em matéria de segurança da informação vão-se generalizando e, como tal, a existência de especificações e normas é crucial. A ausência de normas e especicações acordadas pode constituir uma grande barreira ao avanço dos processos e serviços baseados na informação, na economia e na sociedade. São necessárias acções que acelerem o desenvolvimento e a utilização de tecnologias e normas em diversas áreas ligadas a redes de comunicações e computadores que têm uma importância crítica para utilizadores, indústria e administrações.

4.2 Objectivo

22. São necessários esforços para fornecer meios de suporte e realização de funções específicas nas áreas gerais de OSI, ORE, RDSI/IBC, gestão de redes e segurança de redes para informações não classificadas, mas delicadas. As técnicas e abordagens necessárias para a verificação estão intrinsecamente ligadas à normalização e especificação.

4.3 Situação e tendências

23. Os EUA, em especial, tomaram importantes iniciativas dirigidas à segurança da informação no domínio civil. Na Europa, o assunto é tratado no contexto da normalização das TI e telecomunicações no âmbito do ETSI e do CEN/CENELEC, na preparação de trabalhos do CCITT e da ISO neste domínio.

24. Dadas a preocupações crescentes, os trabalhos nos EUA estão a intensificar-se rapidamente e tanto vendedores cvomo prestadores de serviços estão a aumentar os seus esforços neste domínio. Na Europa, a França, a República Federal da Alemanha e o Reino Unido iniciaram, independentemente, actividades similares, mas só lentamente se está a desenvolver um esforço comum correspondente ao verificado nos EUA.

4.4 Necessidades, Opções e Prioridades

25. Na segurança da informação existe uma relação intrinsicamente muito estreita entre os aspectos de regulamentação, operacionais, administrativos e técnicos. As regulamentações devem reflectir-se nas normas e as disposições relativas à segurança da informação devem satisfazer, de forma verificável, as normas e regulamentações. As regulamentações exigem, em vários aspectos, especificações que ultrapassam o âmbito convencional da normalização, ou seja, incluem códigos de conduta. As exigências em matéria de normas e códigos de conduta estão presentes em todas as áreas da segurança da informação, devendo fazer-se uma distinção entre as exigências de protecção que correspondem aos objectivos de segurança e algumas das exigências técnicas que podem ser confiadas aos organismos de normalização competentes europeus (CEN/CENELEC/ETSI).

26. As especificações e normas devem abranger os domínios dos serviços de segurança da informação (autenticação de pessoas e empresas, protocolos de não repúdio, prova electrónica juridicamente aceitável, controlo da autorização), dos serviços de comunicação (privacidade na comunicação de imagens, privacidade nas comunicações móveis de voz e dados, protecção de bases de dados e de imagens, segurança dos serviços integrados), da gestão da comunicação e segurança (sistema de chaves públicas/privadas para funcionamento de redes abertas, protecção da gestão da rede, protecção do prestador de serviços) e da certificação (critérios e níveis de garantia da segurança da informação, procedimentos de garantia da segurança).

5. Linha de Acção V - Desenvolvimentos Tecnológicos e Operacionais no campo da Segurança da Informação

5.1 Tema

27. O estudo e o desenvolvimento sistemáticos da tecnologia a fim de possibilitar soluções economicamente viáveis e funcionalmente satisfatórias para uma gama de exigências actuais e futuras no domínio da segurança da informação constituem um pré-requisito para o desenvolvimento do mercado de serviços e da competitividade da economia europeia no seu conjunto.

28. Quaisquer desenvolvimentos tecnológicos na segurança dos sistemas da informação terão que incluir simultaneamente os aspectos de segurança dos computadores e segurança das comunicações, dado que a maioria dos sistemas actuais são sistemas distribuídos, obtendo-se o acesso a estes sistemas através de serviços de comunicações.

5.2 Objectivo

29. Estudo e desenvolvimento sistemáticos da tecnologia a fim de possibilitar soluções economicamente viáveis e funcionalmente satisfatórias para uma gama de exigências actuais e futuras no domínio da segurança da informação.

5.3 Necessidades, Opções e Prioridades

30. Os trabalhos em matéria de segurança da informação deverão abordar estratégias de desenvolvimento e realização, tecnologias e ainda integração e verificação.

31. Os trabalhos de I&D estratégica deveriam abordar modelos conceptuais de sistemas seguros (segurança sem compromisso), modelos de exigências funcionais, modelos de riscos e arquitecturas para a segurança.

32. Os trabalhos de I&D orientada para a tecnologia deveriam incluir autenticação do utilizador e da mensagem (por exemplo, através da análise da voz e de assinaturas electrónicas), interfaces e protocolos técnicos para cifragem, mecanismos de controlo de acesso e métodos de realização de sistemas seguros comprováveis.

33. Através de projectos de integração e verificação deveria estudar-se a verificação e validação da segurança técnica dos sistemas e sua aplicabilidade.

34. Para além da consolidação e desenvolvimento da tecnologia da segurança, são necessárias diversas medidas de acompanhamento ligadas à criação, manutenção e aplicação consistente de normas e à validação e certificação de produtos das TI e telecomunicações no que respeita às suas propriedades de segurança, incluindo métodos de validação e certificação na concepção e realização de sistemas.

35. O terceiro programa-quadro comunitário para a IDT poderá ser utilizado para promover projectos de cooperação nos níveis pré-competitivo e pré-normativo.

6. Linha de Acção VI - Oferta de Segurança da Informação

6.1 Tema

36. Em função da natureza exacta das características da segurança da informação, deverão incorporar-se as necessárias funções nas diferentes partes dos sistemas de comunicação, incluindo terminais/computadores, serviços, gestão da rede até aos dispositivos criptográficos, cartões inteligentes, chaves públicas e privadas, etc. Algumas destas partes estarão, previsivelmente, incorporadas nos equipamentos ou suportes lógicos fornecidos pelos vendedores, enquanto outras podem fazer parte de sistemas distribuídos (por exemplo, gestão da rede), estar na posse dos utilizadores individuais (por exemplo, cartões inteligentes) ou ser fornecidas por uma organização especializada (por exemplo, chaves públicas/privadas).

37. A maior parte dos produtos e serviços de segurança da informação podem, previsivelmente, ser fornecidos por vendedores, prestadores de serviços ou operadores. Para funções específicas, por exemplo, oferta de chaves públicas/privadas, auditoria ou autorização, pode vir a ser necessário identificar e mandatar organizações adequadas.

38. O mesmo se aplica a certificação, avaliação e verificação da qualidade do serviço, funções que devem estar a cargo de organizações independentes dos interesses de vendedores, prestadores de serviços ou operadores. Estas organizações poderão ser privadas, públicas ou mandatadas pelo Estado para exercer funções por delegação.

6.2 Objectivo

39. Para facilitar o desenvolvimento harmonioso da oferta de segurança da informação na Comunidade para protecção do público e dos interesses comerciais, será necessário desenvolver uma abordagem coerente da oferta de segurança da informação. Sempre que haja necessidade de mandatar organizações independentes, as suas funções e condições de funcionamento deverão ser definidas, acordadas e, se necessário, incluídas no quadro regulamentar. O objectivo será a obtenção de uma repartição de responsabilidades claramente definida e acordada entre os diferentes intervenientes a nível comunitário, como pré-requisito para o reconhecimento mútuo.

6.3 Situação e tendências

40. Actualmente a oferta de segurança da informação está bem organizada apenas em áreas específicas e limitada à resposta a necessidades específicas. A organização a nível europeu é, em geral, informal e o reconhecimento mútuo da verificação e certificação ainda não existe fora de grupos fechados. Com a crescente importância da segurança da informação, a necessidade de definição de uma abordagem coerente da oferta de segurança da informação a nível europeu e internacional está a tornar-se urgente.

6.4 Necessidades, opções e prioridades

41. Dado o número de intervenientes envolvidos e as relações estreitas com questões de regulamentação e legislativas, é especialmente importante chegar-se a um acordo prévio sobre os princípios que devem reger a oferta de segurança da informação. Ao desenvolver-se uma abordagem coerente deste problema, há que tratar dos aspectos de identificação e especificação de funções que exigem, pela sua natureza, a existência de uma organização independente (ou organizações que trabalhem em conjunto). Tal poderia

abranger funções como a administração de um sistema de chaves públicas/privadas. Além disso, é necessário identificar e especificar, desde logo, as funções que, no interesse público, devem ser confiadas a uma organização independente (ou organizações que trabalhem em conjunto). Poderá aqui incluir-se, por exemplo, auditoria, garantia da qualidade, verificação, certificação e funções similares.

FINANCIAL STATEMENT

Information Security (INFOSEC)
Preparatory Action

BUDGET HEADING

Subsection B6, Item 8104

2. LEGAL BASE AND PROPOSED CLASSIFICATION

Article [235]

Non compulsory expenditure.

3. DESCRIPTION

Collaboration in the development of proposals and actions relating to information security as far as they require or significantly benefit from a concerted approach at Community level. The focus of the work is to relate to the needs of the general public, commerce, service providers and administrations and addresses the requirements for a collaborating approach to technological research, standardisation and related issues as relevant for the development or a consistent European approach to information security with particular reference to the completion of the internal market in 1992.

The goal of the INFOSEC action is to make a major contribution to the objective of the

"development of actions to providing effective and practical security for information held in an electronic form to the general users, administrations and business community without compromising the interest of the public at large."

The present proposal is the result of the preliminary investigations by experts, consultations and on-going related work.

The scope of the preparatory action is to focus on

I. development of an information security strategy framework
II. information security requirements
III. solutions for immediate and interim needs
IV. specifications, standardisation and verification of information security
V. technological and operational developments for information security
VI. information security provision.

4. JUSTIFICATION

Development of a harmonised approach to information security must form an integral part of the Community policies related to the completion of the Internal Market, strengthening of socio-economic performance and international competitiveness. It is vital that Information Security does not become a constraint to the promotion of harmonious development in the Community and to relations with other countries. In addition, information security systems must protect privacy, intellectual property, fair competition, national security and other interests.

The proposed action responds to an urgent need to facilitate and accelerate the emergence of generally accepted, effective and practicable measures in information security. The action will benefit from synergies with on-going programmes in the field of information technologies (ESPRIT) and telecommunications (RACE) as well as the on-going work on telecommunications, standardisation and information market policies.

5. INDICATIVE FINANCIAL PLANNING

5.0 *Implications for expenditure.*

5.0.0 Total cost over the whole of the expected duration of 2 years (in MioECU):

From the Budget of the Communities:	12.0
From the other sectors at the national level:	0.0
TOTAL	12.0

5.0.1 Multi-annual schedule (in MioECU):

	Commitment Appropriations	Payment Appropriations
1991	6	4
1992	6	6
1993	-	2
	12	12

5.0.2 Method of calculation

a) Expenditure by contract

This expenditure covers the Community's financial contribution to analytical work as required to support the development of specific actions proposals, the consultation and establishment of consensus.

b) Operational expenditure

Given the fact that the action is financed in Subsection 6 of the budget devoted to Research and Investment expenditure, administrative costs (Committee and working party meetings, consultation of experts, missions, document distribution or dissemination of techniques, use of data processing, telecommunication and broadcasting equipment) are covered directly by the budget item.

The following table fives the indicative breakdown over the various categories of expenditure (in MioECU):

				1991	1992
5.0.2	a)			4,823	4,100
5.0.2	b)		in total	1,177	1,900
of which		Experts		*0,400*	*0,600*
		Other operational expenditure		*0,500*	*0,725*
		Infrastructure		*0,050*	*0,100*
		Information and publication		*0,050*	*0,100*
		Statutory staff		*0,177*	*0,375*

6. FINANCIAL IMPLICATIONS FOR STAFF AND CURRENT ADMINISTRATIVE APPROPRIATIONS

The statutory research staff involved, i.e. 3 A, 1 B, 1 C, will be entered in the research staff table and is paid out of the appropriations entered onto Item B6-8104.

The administrative expenditure will be governed by the internal rules on mini-budgets decided by the Commission on 22 May 1990.

FINANCING OF EXPENDITURE

The appropriations to cover the Community's contribution to this project will be determined in the context of the annual budgetary procedure.

IMPLICATIONS FOR REVENUE

Contribution of the statutory research staff to the retirement scheme and the sickness insurance.

9. TYPE OF CONTROL

- Administrative control by the Director General for Financial Control as regards budget implementation;
- Control of achievement:
  - SOG-IS
  - control by officials of the Commission
  - audit by the Court of Auditors in accordance with provisions of the Treaty;
- In accordance with Article 2 of the Financial Regulations, the use of appropriations will be subject to analyses of cost-effectiveness and the realisation of quantified objectives will be monitored.