COLETÂNEA DE LEGISLAÇÃO

PROTEÇÃO DE DADOS PESSOAIS

CCA ONTIER

WWW.CCA-ONTIER.COM

CCA
ADVOGADOS

ONTIER

PROTEÇÃO DE DADOS PESSOAIS

COLETÂNEA DE LEGISLAÇÃO

2015

ÍNDICE

1 - Lei nº 67/98 de 26 de Outubro, Lei da Proteção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Diretiva nº95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados)

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º Objeto
A presente lei transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 2.º Princípio geral
O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.

Artigo 3.º Definições
Para efeitos da presente lei, entende-se por:

a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

b) «Tratamento de dados pessoais» («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

c) «Ficheiro de dados pessoais» («ficheiro»): qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

d) «Responsável pelo tratamento»: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa;

e) «Subcontratante»: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento;

f) «Terceiro»: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados;

g) «Destinatário»: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal;

h) «Consentimento do titular dos dados»: qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento;

i) «Interconexão de dados»: forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade.

Artigo 4.º Âmbito de aplicação

1. A presente lei aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados.

2. A presente lei não se aplica ao tratamento de dados pessoais efetuado por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.

3. A presente lei aplica-se ao tratamento de dados pessoais efetuado:
a) No âmbito das atividades de estabelecimento do responsável do tratamento situado em território português;

b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional;

c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia.

4. A presente lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português.

5. No caso referido na alínea c) do n.º 3, o responsável pelo tratamento deve designar, mediante comunicação à Comissão Nacional de Proteção de Dados (CNPD), um representante estabelecido em Portugal, que se lhe substitua em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade.

6. O disposto no número anterior aplica-se no caso de o responsável pelo tratamento estar abrangido por estatuto de extraterritorialidade, de imunidade ou por qualquer outro que impeça o procedimento criminal.

7. A presente lei aplica-se ao tratamento de dados pessoais que tenham por objetivo a segurança pública, a defesa nacional e a segurança do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que Portugal se vincule e de legislação específica atinente aos respetivos setores.

CAPÍTULO II
TRATAMENTO DE DADOS PESSOAIS

Secção I
QUALIDADE DOS DADOS E LEGITIMIDADE DO SEU TRATAMENTO

Artigo 5.º Qualidade dos dados

1. Os dados pessoais devem ser:

a) Tratados de forma lícita e com respeito pelo princípio da boa fé;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;

c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;

d) Exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;

e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

2. Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea e) do número anterior.

3. Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores.

Artigo 6.º Condições de legitimidade do tratamento de dados
O tratamento de dados pessoais só pode ser efetuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:
a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

Artigo 7.º Tratamento de dados sensíveis
1. É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

2. Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º

3. O tratamento dos dados referidos no n.º 1 é ainda permitido quando se verificar uma das seguintes condições:
a) Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

b) Ser efetuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

c) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

d) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efetuado exclusivamente com essa finalidade.

4. O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação.

Artigo 8.º Suspeitas de atividades ilícitas,
infrações penais e contraordenações
1. A criação e a manutenção de registos centrais relativos a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só podem ser mantidas por serviços públicos com competência específica prevista na respetiva lei de organização e funcionamento, observando normas procedimentais e de proteção de dados previstas em diploma legal, com prévio parecer da CNPD.

2. O tratamento de dados pessoais relativos a suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela CNPD, observadas as normas de proteção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados.

3. O tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infração determinada, para o exercício de competências previstas no respetivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte.

Artigo 9.º Interconexão de dados pessoais
1. A interconexão de dados pessoais que não esteja prevista em disposição legal está sujeita a autorização da CNPD solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no artigo 27.º

2. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, não implicar discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, ser rodeada de adequadas medidas de segurança e ter em conta o tipo de dados objeto de interconexão.

SECÇÃO III
SEGURANÇA E CONFIDENCIALIDADE DO TRATAMENTO

Artigo 14.º Segurança do tratamento
1. O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua

aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

2. O responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efetuar, e deverá zelar pelo cumprimento dessas medidas.

3. A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou ato jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que o subcontratante apenas a tua mediante instruções do responsável pelo tratamento e que lhe incumbe igualmente o cumprimento das obrigações referidas no n.º 1.

4. Os elementos de prova da declaração negocial, do contrato ou do ato jurídico relativos à proteção dos dados, bem como as exigências relativas às medidas referidas no n.º 1, são consignados por escrito em documento em suporte com valor probatório legalmente reconhecido.

Artigo 15.º Medidas especiais de segurança

1. Os responsáveis pelo tratamento dos dados referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º devem tomar as medidas adequadas para:

a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);

b) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);

c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);

d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);

e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);

f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão);
g) Garantir que possa verificar-se a posteriori, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos quando e por quem (controlo da introdução);

h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

2. Tendo em conta a natureza das entidades responsáveis pelo tratamento e o tipo das instalações em que é efetuado, a CNPD pode dispensar a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos, liberdades e garantias dos titulares dos dados.

3. Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais.

4. A CNPD pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 7.º e 8.º possa pôr em risco direitos, liberdades e garantias dos respetivos titulares, a transmissão seja cifrada.

Artigo 16.º Tratamento por subcontratante
Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais não pode proceder ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais.

Artigo 17.º Sigilo profissional
1. Os responsáveis do tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

2. Igual obrigação recai sobre os membros da CNPD, mesmo após o termo do mandato.3. O disposto nos números anteriores não exclui o dever do fornecimento das informações obrigatórias, nos termos legais, exceto quando constem de ficheiros organizados para fins estatísticos.
4. Os funcionários, agentes ou técnicos que exerçam funções de assessoria à CNPD ou aos seus vogais estão sujeitos à mesma obrigação de sigilo profissional.

CAPÍTULO III
TRANSFERÊNCIA DE DADOS PESSOAIS

SECÇÃO I
TRANSFERÊNCIA DE DADOS PESSOAIS NA UNIÃO EUROPEIA

Artigo 18.º Princípio
É livre a circulação de dados pessoais entre Estados membros da União Europeia, sem prejuízo do disposto nos atos comunitários de natureza fiscal e aduaneira.

SECÇÃO II
TRANSFERÊNCIA DE DADOS PESSOAIS PARA FORA DA UNIÃO EUROPEIA

Artigo 19.º Princípios
1. Sem prejuízo do disposto no artigo seguinte, a transferência, para um Estado que não pertença à União Europeia, de dados pessoais que sejam objeto de tratamento ou que se destinem a sê-lo só pode realizar-se com o respeito das disposições da presente lei e se o Estado para onde são transferidos assegurar um nível de proteção adequado.

2. A adequação do nível de proteção num Estado que não pertença

à União Europeia é apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, devem ser tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no Estado em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado.

3. Cabe à CNPD decidir se um Estado que não pertença à União Europeia assegura um nível de proteção adequado.

4. A CNPD comunica, através do Ministério dos Negócios Estrangeiros, à Comissão Europeia os casos em que tenha considerado que um Estado não assegura um nível de proteção adequado.

5. Não é permitida a transferência de dados pessoais de natureza idêntica aos que a Comissão Europeia tiver considerado que não gozam de proteção adequada no Estado a que se destinam.

Artigo 20.º Derrogações

1. A transferência de dados pessoais para um Estado que não assegure um nível de proteção adequado na aceção do n.º 2 do artigo 19.º pode ser permitida pela CNPD se o titular dos dados tiver dado de forma inequívoca o seu consentimento à transferência ou se essa transferência:

a) For necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

b) For necessária para a execução ou celebração de um contrato celebrado ou a celebrar, no interesse do titular dos dados, entre o responsável pelo tratamento e um terceiro; ou

c) For necessária ou legalmente exigida para a proteção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou

d) For necessária para proteger os interesses vitais do titular dos dados; ou

e) For realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2. Sem prejuízo do disposto no n.º 1, a CNPD pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um Estado que não assegure um nível de proteção adequado na aceção do n.º 2 do artigo 19.º desde que o responsável pelo tratamento assegure mecanismos suficientes de garantia de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do seu exercício, designadamente, mediante cláusulas contratuais adequadas.

3. A CNPD informa a Comissão Europeia, através do Ministério dos Negócios Estrangeiros, bem como as autoridades competentes dos restantes Estados da União Europeia, das autorizações que conceder nos termos do n.º 2.

4. A concessão ou derrogação das autorizações previstas no n.º 2 efetua-se pela CNPD nos termos de processo próprio e de acordo com as decisões da Comissão Europeia.

5. Sempre que existam cláusulas contratuais tipo aprovadas pela Comissão Europeia, segundo procedimento próprio, por oferecerem as garantias suficientes referidas no n.º 2, a CNPD autoriza a transferência de dados pessoais que se efetue ao abrigo de tais cláusulas.

6. A transferência de dados pessoais que constitua medida necessária à proteção da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação e repressão das infrações penais é regida por disposições legais específicas ou pelas convenções e acordos internacionais em que Portugal é parte.

CAPÍTULO IV
COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

SECÇÃO I
NATUREZA, ATRIBUIÇÕES E COMPETÊNCIAS

Artigo 21.º Natureza
1. A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República.

2. A CNPD, independentemente do direito nacional aplicável a cada tratamento de dados em concreto exerce as suas competências em todo o território nacional.

3. A CNPD pode ser solicitada a exercer os seus poderes por uma autoridade de controlo de proteção de dados de outro Estado membro da União Europeia ou do Conselho da Europa.
4. A CNPD coopera com as autoridades de controlo de proteção de dados de outros Estados na difusão do direito e das regulamentações nacionais em matéria de proteção de dados pessoais, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Artigo 22.º Atribuições
1. A CNPD é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.

2. A CNPD deve ser consultada sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias ou internacionais, relativos ao tratamento de dados pessoais.

3. A CNPD dispõe:
a) De poderes de investigação e de inquérito, podendo aceder aos dados objeto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo;

b) De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português;

c) Do poder de emitir pareceres prévios ao tratamento de dados pessoais, assegurando a sua publicitação.

4. Em caso de reiterado não cumprimento das disposições legais em matéria de dados pessoais, a CNPD pode advertir ou censurar publicamente o responsável pelo tratamento, bem como suscitar a questão, de acordo com as respetivas competências, à Assembleia da República, ao Governo ou a outros órgãos ou autoridades.

5. A CNPD tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei e deve denunciar ao Ministério Público as infrações penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de prova.

6. A CNPD é representada em juízo pelo Ministério Público e está isenta de custas nos processos em que intervenha.

Artigo 23.º Competências
1. Compete em especial à CNPD:
a) Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais;

b) Autorizar ou registar, consoante os casos, os tratamentos de dados pessoais;

c) Autorizar excecionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5.º;

d) Autorizar, nos casos previstos no artigo 9.º, a interconexão de tratamentos automatizados de dados pessoais;

e) Autorizar a transferência de dados pessoais nos casos previstos no artigo 20.º;

f) Fixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir diretivas para determinados sectores de atividade;

g) Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de retificação e atualização;

h) Autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, bem como fixar os prazos máximos de cumprimento, em cada sector de atividade, das obrigações que, por força dos artigos 11.º a 13.º, incumbem aos responsáveis pelo tratamento de dados pessoais;

i) Dar seguimento ao pedido efetuado por qualquer pessoa, ou por associação que a represente, para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais e informá-la do resultado;

j) Efetuar, a pedido de qualquer pessoa, a verificação de licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;

k) Apreciar as reclamações, queixas ou petições dos particulares;

l) Dispensar a execução de medidas de segurança, nos termos previstos no n.º 2 do artigo 15.º, podendo emitir diretivas para determinados sectores de atividade;

m) Assegurar a representação junto de instâncias comuns de controlo e em reuniões comunitárias e internacionais de entidades independentes de controlo da proteção de dados pessoais, bem como

participar em reuniões internacionais no âmbito das suas competências, designadamente exercer funções de representação e fiscalização no âmbito dos sistemas Schengen e Europol, nos termos das disposições aplicáveis;

n) Deliberar sobre a aplicação de coimas;

o) Promover e apreciar códigos de conduta;

p) Promover a divulgação e esclarecimento dos direitos relativos à proteção de dados e dar publicidade periódica à sua atividade, nomeadamente através da publicação de um relatório anual;

q) Exercer outras competências legalmente previstas.

2. No exercício das suas competências de emissão de diretivas ou de apreciação de códigos de conduta, a CNPD deve promover a audição das associações de defesa dos interesses em causa.

3. No exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e de recurso para o Tribunal Central Administrativo.

4. A CNPD pode sugerir à Assembleia da República as providências que entender úteis à prossecução das suas atribuições e ao exercício das suas competências.

Artigo 24.º Dever de colaboração
1. As entidades públicas e privadas devem prestar a sua colaboração à CNPD, facultando-lhe todas as informações que por esta, no exercício das suas competências, lhes forem solicitadas.

2. O dever de colaboração é assegurado, designadamente, quando a CNPD tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.

3. A CNPD ou os seus vogais, bem como os técnicos por ela mandatados, têm direito de acesso aos sistemas informáticos que sirvam de suporte ao tratamento dos dados, bem como à documentação referida no número anterior, no âmbito das suas atribuições e competências.

SECÇÃO II
COMPOSIÇÃO E FUNCIONAMENTO

Artigo 25.º Composição e mandato

1. A CNPD é composta por sete membros de integridade e mérito reconhecidos, dos quais o presidente e dois dos vogais são eleitos pela Assembleia da República segundo o método da média mais alta de Hondt.

2. Os restantes vogais são:

a) Dois magistrados com mais de 10 anos de carreira, sendo um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público;

b) Duas personalidades de reconhecida competência designadas pelo Governo.

3. O mandato dos membros da CNPD é de cinco anos e cessa com a posse dos novos membros.

4. Os membros da CNPD constam de lista publicada na 1.ª série do Diário da República.

5. Os membros da CNPD tomam posse perante o Presidente da Assembleia da República nos 10 dias seguintes à publicação da lista referida no número anterior.

Artigo 26.º Funcionamento

1. São aprovados por lei da Assembleia da República:

a) A lei orgânica e o quadro de pessoal da CNPD;

b) O regime de incompatibilidades, de impedimentos, de suspeições e de perda de mandato, bem como o estatuto remuneratório dos membros da CNPD.

2. O estatuto dos membros da CNPD garante a independência do exercício das suas funções.

3. A Comissão dispõe de quadro próprio para apoio técnico e administrativo, beneficiando os seus funcionários e agentes do estatuto e regalias do pessoal da Assembleia da República.

SECÇÃO III
NOTIFICAÇÃO

Artigo 27.º Obrigação de notificação à CNPD
1. O responsável pelo tratamento ou, se for caso disso, o seu representante deve notificar a CNPD antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados à prossecução de uma ou mais finalidades interligadas.

2. A CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, atendendo aos dados a tratar, não sejam suscetíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência.

3. A autorização, que está sujeita a publicação no Diário da República, deve especificar as finalidades do tratamento, os dados ou categorias de dados a tratar a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.

4. Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem a informação do público e possam ser consultados pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.

5. Os tratamentos não automatizados dos dados pessoais previstos no n.º 1 do artigo 7.º estão sujeitos a notificação quando tratados ao abrigo da alínea a) do n.º 3 do mesmo artigo.

Artigo 28.º Controlo prévio
1. Carecem de autorização da CNPD:
a) O tratamento dos dados pessoais a que se referem o n.º 2 do artigo 7.º e o n.º 2 do artigo 8.º;

b) O tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares;

c) A interconexão de dados pessoais prevista no artigo 9.º;

d) A utilização de dados pessoais para fins não determinantes da recolha.

2. Os tratamentos a que se refere o número anterior podem ser autorizados por diploma legal, não carecendo neste caso de autorização da CNPD.

Artigo 29.º Conteúdo dos pedidos de parecer ou de autorização e da notificação
Os pedidos de parecer ou de autorização, bem como as notificações, remetidos à CNPD devem conter as seguintes informações:
a) Nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;

b) As finalidades do tratamento;

c) Descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem;

d) Destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;

e) Entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;

f) Eventuais interconexões de tratamentos de dados pessoais;

g) Tempo de conservação dos dados pessoais;

h) Forma e condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem;

i) Transferências de dados previstas para países terceiros;

j) Descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação dos artigos 14.º e 15.º

Artigo 30.º Indicações obrigatórias
1. Os diplomas legais referidos no n.º 2 do artigo 7.º e no n.º 1 do artigo 8.º, bem como as autorizações da CNPD e os registos de tratamentos de dados pessoais, devem, pelo menos, indicar:
a) O responsável do ficheiro e, se for caso disso, o seu representante;

b) As categorias de dados pessoais tratados;

c) As finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;

d) A forma de exercício do direito de acesso e de retificação;

e) Eventuais interconexões de tratamentos de dados pessoais;

f) Transferências de dados previstas para países terceiros.

2. Qualquer alteração das indicações constantes do n.º 1 está sujeita aos procedimentos previstos nos artigos 27.º e 28.º

Artigo 31.º Publicidade dos tratamentos
1. O tratamento dos dados pessoais, quando não for objeto de diploma legal e dever ser autorizado ou notificado, consta de registo na CNPD, aberto à consulta por qualquer pessoa.

2. O registo contém as informações enumeradas nas alíneas a) a d) e i) do artigo 29.º

3. O responsável por tratamento de dados não sujeito a notificação está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite, pelo menos as informações referidas no n.º 1 do artigo 30.º

4. O disposto no presente artigo não se aplica a tratamentos cuja única

finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem à informação do público e se encontrem abertos à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo.

5. A CNPD deve publicar no seu relatório anual todos os pareceres e autorizações elaborados ou concedidas ao abrigo da presente lei, designadamente as autorizações previstas no n.º 2 do artigo 7.º e no n.º 2 do artigo 9.º

CAPÍTULO V
CÓDIGOS DE CONDUTA

Artigo 32.º Códigos de conduta
1. A CNPD apoia a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes sectores, para a boa execução das disposições da presente lei.

2. As associações profissionais e outras organizações representativas de categorias de responsáveis pelo tratamento de dados que tenham elaborado projetos de códigos de conduta podem submetê-los à apreciação da CNPD.

3. A CNPD pode declarar a conformidade dos projetos com as disposições legais e regulamentares vigentes em matéria de proteção de dados pessoais.

CAPÍTULO VI
TUTELA ADMINISTRATIVA E JURISDICIONAL

SECÇÃO I
TUTELA ADMINISTRATIVA E JURISDICIONAL

Artigo 33.º Tutela administrativa e jurisdicional
Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos

ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de proteção de dados pessoais.

Artigo 34.º Responsabilidade civil
1. Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições legais em matéria de proteção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido.

2. O responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

SECÇÃO II
CONTRAORDENAÇÕES

Artigo 35.º Legislação subsidiária
Às infrações previstas na presente secção é subsidiariamente aplicável o regime geral das contraordenações, com as adaptações constantes dos artigos seguintes.

Artigo 36.º Cumprimento do dever omitido
Sempre que a contraordenação resulte de omissão de um dever, a aplicação da sanção e o pagamento da coima não dispensam o infrator do seu cumprimento, se este ainda for possível.

Artigo 37.º Omissão ou defeituoso cumprimento de obrigações
1. As entidades que, por negligência, não cumpram a obrigação de notificação à CNPD do tratamento de dados pessoais a que se referem os n.ºs 1 e 5 do artigo 27.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 29.º, ou ainda quando, depois de notificadas pela CNPD, mantiverem o acesso às redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contraordenação punível com as seguintes coimas:
a) Tratando-se de pessoa singular, no mínimo de 50 000$00 e no máximo de 500 000$00[1];

[1] *€ 249,40 a € 2.493,99.*

b) Tratando-se de pessoa coletiva ou de entidade sem personalidade jurídica, no mínimo de 300 000$00 e no máximo de 3 000 000$00[2].

2. A coima é agravada para o dobro dos seus limites quando se trate de dados sujeitos a controlo prévio, nos termos do artigo 28.º.

Artigo 38.º Contraordenações
1. Praticam contraordenação punível com a coima mínima de 100 000$00 e máxima de 1 000 000$00[3], as entidades que não cumprirem alguma das seguintes disposições da presente lei:
a) Designar representante nos termos previstos no n.º 5 do artigo 4.º;

b) Observar as obrigações estabelecidas nos artigos 5.º, 10.º, 11.º, 12.º, 13.º, 15.º, 16.º e 31.º, n.º 3.

2. A pena é agravada para o dobro dos seus limites quando não forem cumpridas as obrigações constantes dos artigos 6.º, 7.º, 8.º, 9.º, 19.º e 20.º

Artigo 39.º Concurso de infrações
1. Se o mesmo facto constituir, simultaneamente, crime e contraordenação, o agente é punido sempre a título de crime.

2. As sanções aplicadas às contraordenações em concurso são sempre cumuladas materialmente.

Artigo 40.º Punição de negligência e da tentativa
1. A negligência é sempre punida nas contraordenações previstas no artigo 38.º

2. A tentativa é sempre punível nas contraordenações previstas nos artigos 37.º e 38.º

Artigo 41.º Aplicação das coimas
1. A aplicação das coimas previstas na presente lei compete ao presidente da CNPD, sob prévia deliberação da Comissão.

---

[2] € 1.496.39 a € 14.963,86.
[3] € 498,80 a € 4.987,98.

2. A deliberação da CNPD, depois de homologada pelo presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

Artigo 42.º Destino das receitas cobradas
O montante das importâncias cobradas, em resultado da aplicação das coimas, reverte, em partes iguais, para o Estado e para a CNPD.

SECÇÃO III
CRIMES

Artigo 43.º Não cumprimento de obrigações relativas a proteção de dados
1. É punido com prisão até um ano ou multa até 120 dias quem intencionalmente:
a) Omitir a notificação ou o pedido de autorização a que se referem os artigos 27.º e 28.º;

b) Fornecer falsas informações na notificação ou nos pedidos de autorização para o tratamento de dados pessoais ou neste proceder a modificações não consentidas pelo instrumento de legalização;

c) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização;

d) Promover ou efetuar uma interconexão ilegal de dados pessoais;

e) Depois de ultrapassado o prazo que lhes tiver sido fixado pela CNPD para cumprimento das obrigações previstas na presente lei ou em outra legislação de proteção de dados, as não cumprir;

f) Depois de notificado pela CNPD para o não fazer, mantiver o acesso a redes abertas de transmissão de dados a responsáveis pelo tratamento de dados pessoais que não cumpram as disposições da presente lei.

2. A pena é agravada para o dobro dos seus limites quando se tratar d% dados pessoais a que se referem os artigos 7.º e 8.º

Artigo 44.º Acesso indevido
1. Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado é punido com prisão até um ano ou multa até 120 dias.

2. A pena é agravada para o dobro dos seus limites quando o acesso:
a) For conseguido através de violação de regras técnicas de segurança;

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;

c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

3. No caso do n.º 1 o procedimento criminal depende de queixa.

Artigo 45.º Viciação ou destruição de dados pessoais
1. Quem, sem a devida autorização, apagar, destruir, danificar, suprimirou modificar dados pessoais, tornando-os inutilizáveis ou afetando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias.

2. A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

3. Se o agente atuar com negligência, a pena é, em ambos os casos, de prisão até um ano ou multa até 120 dias.

Artigo 46.º Desobediência qualificada
1. Quem, depois de notificado para o efeito, não interromper, cessar ou bloquear o tratamento de dados pessoais é punido com a pena correspondente ao crime de desobediência qualificada.

2. Na mesma pena incorre quem, depois de notificado:
a) Recusar, sem justa causa, a colaboração que concretamente lhe for exigida nos termos do artigo 24.º;

b) Não proceder ao apagamento, destruição total ou parcial de dados pessoais;

c) Não proceder à destruição de dados pessoais, findo o prazo de conservação previsto no artigo 5.º

Artigo 47.º Violação do dever de sigilo
1. Quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias.

2. A pena é agravada de metade dos seus limites se o agente:
a) For funcionário público ou equiparado, nos termos da lei penal;
b) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;

c) Puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

3. A negligência é punível com prisão até seis meses ou multa até 120 dias.

4. Fora dos casos previstos no n.º 2, o procedimento criminal depende de queixa.

Artigo 48.º Punição da tentativa
Nos crimes previstos nas disposições anteriores, a tentativa é sempre punível.

Artigo 49.º Pena acessória
1. Conjuntamente com as coimas e penas aplicadas pode, acessoriamente, ser ordenada:
a) A proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados;

b) A publicidade da sentença condenatória;

c) A advertência ou censura públicas do responsável pelo tratamento, nos termos do n.º 4 do artigo 22.º

2. A publicidade da decisão condenatória faz-se a expensas do condenado, na publicação periódica de maior expansão editada na área da comarca da prática da infração ou, na sua falta, em publicação periódica da comarca mais próxima, bem como através da afixação de edital em suporte adequado, por período não inferior a 30 dias.

3. A publicação é feita por extrato de que constem os elementos da infração e as sanções aplicadas, bem como a identificação do agente.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Artigo 50.º Disposição transitória
1. Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente lei devem cumprir o disposto nos artigos 7.º, 8.º, 10.º e 11.º no prazo de cinco anos.

2. Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a retificação, o apagamento ou o bloqueio dos dados incompletos, inexatos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.

3. A CNPD pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os artigos 7.º, 8.º e 9.º, desde que não sejam em nenhum caso reutilizados para finalidade diferente.

Artigo 51.º Disposição revogatória
São revogadas as Leis n.os10/91, de 29 de Abril, e 28/94, de 29 de Agosto.

Artigo 52.º Entrada em vigor
A presente lei entra em vigor no dia seguinte ao da sua publicação.

Aprovada em 24 de Setembro de 1998.
O Presidente da Assembleia da República,
António de Almeida Santos.
Promulgada em 7 de Outubro de 1998.
Publique-se.
O Presidente da República,
Jorge Sampaio.
Referendada em 14 de Outubro de 1998.
O Primeiro-Ministro,
António Manuel de Oliveira Guterres.

2. Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

O PARLAMENTO EUROPEU O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia e, nomeada-mente, o seu artigo 100º A,

Tendo em conta a proposta da Comissão[4],

Tendo em conta o parecer do Comité Económico e Social[5],

Deliberando nos termos do procedimento previsto no artigo 189º B do Tratado[6],

1 // Considerando que os objetivos da Comunidade, enunciados no Tratado, com a redação que lhe foi dada pelo Tratado da União Europeia, consistem em estabelecer uma união cada vez mais estreita entre os povos europeus, em fomentar relações mais próximas entre os Estados que pertencem à Comunidade, em assegurar o progresso económico e social mediante ações comuns para eliminar as barreiras que dividem a Europa, em promover a melhoria constante das condições de vida dos seus povos, em preservar e consolidar a paz e a liberdade e em promover a democracia com base nos direitos fundamentais reconhecidos nas Constituições e leis dos Estados-membros, bem como na Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais;

2 // Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso

---

[4] JO nº C 277 de 5. 11. 1990, p. 3, e JO nº C 311 de 27. 11. 1992, p. 30

[5] JO nº C 159 de 17. 6. 1991, p. 38.

[6] Parecer do Parlamento Europeu de 11 de Março de 1992 (JO nº C 94 de 13. 4. 1992, p. 198), confirmado em 2 de Dezembro de 1993 (JO nº C 342 de 20. 12. 1993, p. 30), posição comum do Conselho de 20 de Fevereiro de 1995 (JO nº C 93 de 13. 4. 1995, p. 1) e decisão do Parlamento Europeu de 15 de Junho de 1995 (JO nº C 166 de 3. 7. 1995).

económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos;

3 // Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado, é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas;

4 // Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das atividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados;

5 // Considerando que a integração económica e social resultante do estabelecimento e funcionamento do mercado interno nos termos do artigo 7º A do Tratado irá necessariamente provocar um aumento sensível dos fluxos transfronteiras de dados pessoais entre todos os intervenientes, privados ou públicos, na vida económica e social dos Estados-membros; que o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados-membros tende a intensificar-se; que as administrações dos Estados-membros são chamadas, por força do direito comunitário, a colaborar e a trocar entre si dados pessoais a fim de poderem desempenhar as suas atribuições ou executar tarefas por conta de uma administração de outro Estado-membro, no âmbito do espaço sem fronteiras internas que o mercado interno constitui;

6 // Considerando, além disso, que o reforço da cooperação científica bem como a introdução coordenada de novas redes de telecomunicações na Comunidade exigem e facilitam a circulação transfronteiras de dados pessoais;

7 // Considerando que as diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que

estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de atividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de proteção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;

8 // Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objetivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam atualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objetivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma ação comunitária com vista à aproximação das legislações;

9 // Considerando que, devido à proteção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estadas-membros uma margem de manobra que, no contexto da aplicação da diretiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a proteção atualmente assegurada na respetiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da diretiva, o que poderá refletir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade;

10 // Considerando que o objetivo das legislações nacionais relativas ao tratamento de dados pessoais é assegurar o respeito dos direitos

e liberdades fundamentais, nomeadamente do direito à vida privada, reconhecido não só no artigo 8º da Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais como nos princípios gerais do direito comunitário; que, por este motivo, a aproximação das referidas legislações não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na Comunidade;

11 // Considerando que os princípios da proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, contidos na presente diretiva, precisam e ampliam os princípios contidos na Convenção do Conselho da Europa, de 28 de Janeiro de 1981, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais;

12 // Considerando que os princípios da proteção devem aplicar-se a todo e qualquer tratamento de dados pessoais sempre que as atividades do responsável pelo tratamento sejam regidas pelo direito comunitário; que se deve excluir o tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, por exemplo correspondência ou listas de endereços;

13 // Considerando que as atividades referidas nos títulos V e VI do Tratado da União Europeia, relativas à segurança pública, à defesa, à segurança do Estado ou às atividades do Estado no domínio penal, não são abrangidas pelo âmbito de aplicação do direito comunitário, sem prejuízo das obrigações que incumbem aos Estados-membros nos termos do nº 2 do artigo 56º e dos artigos 57º e 100º A do Tratado; que o tratamento de dados pessoais necessário à proteção do bem-estar económico do Estado não é abrangido pela presente diretiva quando esse tratamento disser respeito a questões de segurança do Estado;

14 // Considerando que, tendo em conta a importância do desenvolvimento que, no âmbito da sociedade de informação, sofrem atualmente as técnicas de captação, transmissão, manipulação, gravação, conservação ou comunicação de dados de som e de imagem relativos às pessoas singulares, há que aplicar a presente diretiva ao tratamento desses dados;

15 // Considerando que o tratamento desses dados só é abrangido pela presente diretiva se for automatizado ou se os dados tratados estiverem contidos ou se destinarem a ficheiros estruturados segundo critérios específicos relativos às pessoas, a fim de permitir um acesso fácil aos dados pessoais em causa;

16 // Considerando que o tratamento de dados de som e de imagem, tais como os de vigilância por vídeo, não é abrangido pelo âmbito de aplicação da presente diretiva se for executado para fins de segurança pública, de defesa, de segurança do Estado ou no exercício de atividades do Estado relativas a domínios de direito penal ou no exercício de outras atividades não abrangidas pelo âmbito de aplicação do direito comunitário;

17 // Considerando que, no que se refere ao tratamento de som e de imagem para fins jornalísticos ou de expressão literária ou artística, nomeadamente no domínio do audiovisual, os princípios da diretiva se aplicam de modo restrito de acordo com as disposições referidas no artigo 9º;

18 // Considerando que, a fim de evitar que uma pessoa seja privada da proteção a que tem direito por força da presente diretiva, é necessário que qualquer tratamento de dados pessoais efetuado na Comunidade respeite a legislação de um dos Estados-membros; que, nesse sentido, é conveniente que o tratamento efetuado por uma pessoa que age sob a autoridade do responsável pelo tratamento estabelecido num Estado-membro seja regido pela legislação deste Estado-membro;

19 // Considerando que o estabelecimento no território de um Estado-membro pressupõe o exercício efetivo e real de uma atividade mediante uma instalação estável; que, para o efeito, a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante; que, quando no território de vários Estados-membros estiver estabelecido um único responsável pelo tratamento, em especial através de uma filial, deverá assegurar, nomeadamente para evitar que a legislação seja contornada, que cada um dos estabelecimentos cumpra as obrigações impostas pela legislação nacional aplicável às respetivas atividades;

20 // Considerando que o facto de o tratamento de dados ser da responsabilidade de uma pessoa estabelecida num país terceiro não deve constituir obstáculo à proteção das pessoas assegurada pela presente diretiva; que, nesses casos, o tratamento deverá ser regido pela legislação do Estado-membro onde se encontram os meios utilizados para o tratamento de dados em causa e que deverão oferecer-se garantias de que os direitos e as obrigações estabelecidos na presente diretiva serão efetivamente respeitados;

21 // Considerando que a presente diretiva não prejudica as regras de territorialidade aplicáveis em matéria de direito penal;

22 // Considerando que os Estados-membros precisarão, na sua legislação ou nas regras de execução adotadas nos termos das presente diretiva, as condições gerais em que o tratamento de dados é lícito; que, nomeadamente, o artigo 5º, conjugado com os artigos 7º e 8º, permite que os Estados-membros estabeleçam, independentemente das regras gerais, condições especiais para o tratamento de dados em sectores específicos e para as diferentes categorias de dados referidas no artigo 8º;

23 // Considerando que os Estados-membros podem assegurar a concretização da proteção das pessoas tanto por uma lei geral relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais, como por leis sectoriais, por exemplo as relativas aos institutos de estatística;

24 // Considerando que a legislação para a proteção das pessoas coletivas relativamente ao tratamento de dados que lhes dizem respeito não é afetada pela presente diretiva;

25 // Considerando que os princípios de proteção devem encontrar expressão, por um lado, nas obrigações que impendem sobre as pessoas, as autoridades públicas, as empresas, os serviços ou outros organismos responsáveis pelo tratamento de dados, em especial no que respeita à qualidade dos dados, à segurança técnica, à notificação à autoridade de controlo, às circunstâncias em que o tratamento pode ser efetuado, e, por outro, nos direitos das pessoas cujos dados são

tratados serem informadas sobre esse tratamento, poderem ter acesso aos dados, poderem solicitar a sua retificação e mesmo, em certas circunstâncias, poderem opor-se ao tratamento;

26 // Considerando que os princípios da proteção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; que os códigos de conduta na aceção do artigo 27º podem ser um instrumento útil para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anónimos e conservados sob uma forma que já não permita a identificação da pessoa em causa;

27 // Considerando que a proteção das pessoas se deve aplicar tanto ao tratamento automatizado de dados como ao tratamento manual; que o âmbito desta proteção não deve, na prática, depender das técnicas utilizadas, sob pena de se correr o sério risco de a proteção poder ser contornada; que, em todo o caso, no que respeita ao tratamento manual, a presente diretiva apenas abrange os ficheiros e não as pastas não estruturadas; que, em particular, o conteúdo de um ficheiro deve ser estruturado de acordo com critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais; que, em conformidade com a definição da alínea c) do artigo 2º, os diferentes critérios que permitem determinar os elementos de um conjunto estruturado de dados pessoais e os diferentes critérios que regem o acesso a esse conjunto de dados podem ser definidos por cada Estado-membro; que as pastas ou conjuntos de pastas, bem como as suas capas, qu não estejam estruturadas de acordo com critérios específicos, de modo algum se incluem no âmbito de aplicação da presente diretiva;

28 // Considerando que qualquer tratamento de dados pessoais deve ser efetuado de forma lícita e leal para com a pessoa em causa; que deve, em especial, incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com o tratamento; que essas finalidades devem ser explícitas e legítimas e ser determinadas

aquando da recolha dos dados; que as finalidades dos tratamentos posteriores à recolha não podem ser incompatíveis com as finalidades especificadas inicialmente;

29 // Considerando que o tratamento posterior de dados pessoais para fins históricos, estatísticos ou científicos não é de modo geral considerado incompatível com as finalidades para as quais os dados foram previamente recolhidos, desde que os Estados-membros estabeleçam garantias adequadas; que tais garantias devem em especial impedir a utilização de dados em apoio de medidas ou de decisões tomadas em desfavor de uma pessoa;

30 // Considerando que, para ser lícito, o tratamento de dados pessoais deve, além disso, ser efetuado com o consentimento da pessoa em causa ou ser necessário para a celebração ou execução de um contrato que vincule a pessoa em causa, ou para o cumprimento de uma obrigação legal, ou para a execução de uma missão de interesse público ou para o exercício da autoridade pública, ou ainda para a realização do interesse legítimo de uma pessoa, desde que os interesses ou os direitos e liberdades da pessoa em causa não prevaleçam; que, em especial, para assegurar o equilíbrio dos interesses em causa e garantir ao mesmo tempo uma concorrência real, os Estados-membros são livres de determinar as condições em que os dados pessoais podem ser utilizados e comunicados a terceiros no âmbito de atividades legítimas de gestão corrente das empresas e outros organismos; que, do mesmo modo, podem precisar as condições em que a comunicação a terceiros de dados pessoais pode ser efetuada para fins de mala direta ou de prospeção feita por uma instituição de solidariedade social ou outras associações ou fundações, por exemplo de carácter político, desde que respeitem as disposições que permitem à pessoa em causa opor-se, sem necessidade de indicar o seu fundamento ou de suportar quaisquer encargos, ao tratamento dos dados que lhe dizem respeito;

31 // Considerando que, do mesmo modo, o tratamento de dados pessoais deve ser considerado lícito quando se destinar a proteger um interesse essencial à vida da pessoa em causa;

32 // Considerando que cabe às legislações nacionais determinar se o responsável pelo tratamento que executa uma missão de interesse

público ou exerce a autoridade pública deve ser uma administração pública ou outra pessoa sujeita ao direito público ou ao direito privado, por exemplo uma associação profissional;

33 // Considerando que os dados suscetíveis, pela sua natureza, de pôr em causa as liberdades fundamentais ou o direito à vida privada só deverão ser tratados com o consentimento explícito da pessoa em causa; que, no entanto, devem ser expressamente previstas derrogações a esta proibição no que respeita a necessidades específicas, designadamente quando o tratamento desses dados for efetuado com certas finalidades ligadas à saúde por pessoas sujeitas por lei à obrigação de segredo profissional ou para as atividades legítimas de certas associações ou fundações que tenham por objetivo permitir o exercício das liberdades fundamentais;

34 // Considerando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social - em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença - e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia, estabelecer garantias adequadas e específicas para a proteção dos direitos fundamentais e da vida privada das pessoas;

35 // Considerando, além disso, que o tratamento de dados pessoais pelas autoridades públicas para a consecução de objetivos consagrados no direito constitucional ou no direito internacional público, em benefício de associações religiosas oficialmente reconhecidas, é efetuado por motivos de interesse público importante;

36 // Considerando que quando, para o exercício de atividades do âmbito eleitoral, o funcionamento do sistema democrático exigir, em certos Estados-membros, que partidos políticos recolham dados sobre a opinião política das pessoas, o tratamento desses dados pode ser autorizado por motivos de interesse público importante, desde que sejam estabelecidas garantias adequadas;

37 // Considerando que o tratamento de dados pessoais para fins jornalísticos ou de expressão artística ou literária, nomeadamente no domínio do audiovisual, deve beneficiar de derrogações ou de restrições a determinadas disposições da presente diretiva, desde que tal seja necessário para conciliar os direitos fundamentais da pessoa com a liberdade de expressão, nomeadamente a liberdade de receber ou comunicar informações, tal como é garantida, nomeadamente pelo artigo 10º da Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais; que, por conseguinte, compete aos Estados-membros estabelecer, tendo em vista a ponderação dos direitos fundamentais, as derrogações e limitações necessárias que se prendam com as medidas gerais em matéria de legalidade do tratamento de dados, as medidas relativas à transferência de dados para países terceiros, bem como com as competências das autoridades de controlo; que tal facto não deverá, no entanto, levar os Estados-membros a prever derrogações às medidas destinadas a garantir a segurança do tratamento de dados; e que deverão igualmente ser atribuídas pelo menos à autoridade de controlo determinadas competências a posteriori, tais como a de publicar periodicamente um relatório ou de recorrer judicialmente;

38 // Considerando que, para que o tratamento de dados seja leal , a pessoa em causa deve poder ter conhecimento da existência dos tratamentos e obter, no momento em que os dados lhe são pedidos, uma informação rigorosa e completa das circunstâncias dessa recolha;

39 // Considerando que por vezes se tratam dados que não foram recolhidos diretamente pelo responsável junto da pessoa em causa; que, além disso, os dados podem ser legitimamente comunicados a um terceiro sem que essa comunicação estivesse prevista na altura da recolha dos dados junto da pessoa em causa; que, em todos estes casos, a pessoa em causa deve ser informada no momento do registo dos dados ou, o mais tardar, quando os dados são comunicados pela primeira vez a um terceiro;

40 // Considerando que, no entanto, a imposição desta obrigação não é necessária caso a pessoa em causa esteja já informada; que, além disso, não existe essa obrigação caso o registo ou a comunicação dos dados

estejam expressamente previstos na lei ou caso a informação da pessoa em causa se revele impossível ou exija esforços desproporcionados, o que pode ser o caso do tratamento para fins históricos, estatísticos ou científicos; que, para este efeito, podem ser tomados em consideração o número de pessoas em causa, a antiguidade dos dados e as medidas compensatórias que podem ser tomadas;

41 // Considerando que todas as pessoas devem poder beneficiar do direito de acesso aos dados que lhes dizem respeito e que estão em fase de tratamento, a fim de assegurarem, nomeadamente, a sua exatidão e a licitude do tratamento; que, pelas mesmas razões, todas as pessoas devem, além disso, ter o direito de conhecer a lógica subjacente ao tratamento automatizado dos dados que lhe dizem respeito, pelo menos no caso das decisões automatizadas referidas no nº 1 do artigo 15º; que este último direito não deve prejudicar o segredo comercial nem a propriedade intelectual, nomeadamente o direito de autor que protege o suporte lógico; que tal, todavia, não poderá traduzir-se pela recusa de qualquer informação à pessoa em causa;

42 // Considerando que, no interesse da pessoa em causa ou com o objetivo de proteger os direitos e liberdades de outrem, os Estados-membros podem limitar os direitos de acesso e de informação; que, por exemplo, podem precisar que o acesso aos dados médicos só poderá ser obtido por intermédio de um profissional da saúde;

43 // Considerando que restrições aos direitos de acesso e informação e a certas obrigações do responsável pelo tratamento podem igualmente ser previstas pelos Estados-membros na medida em que sejam necessárias para proteger, por exemplo, a segurança do Estado, a defesa, a segurança pública, os interesses económicos ou financeiros importantes de um Estado-membro ou da União, e para a investigação e a repressão de infrações penais ou de violações da deontologia das profissões regulamentadas; que há que enumerar, a título das exceções e restrições, as missões de controlo, de inspeção ou de regulamentação necessárias nos três últimos domínios citados referentes à segurança pública, ao interesse económico ou financeiro e à repressão penal; que esta enumeração de missões respeitante aos três domínios referidos não prejudica a legitimidade de exceções e de restrições por razões de segurança do Estado e de defesa;

44 // Considerando que os Estados-membros podem ser levados, por força das disposições do direito comunitário, a prever derrogações às disposições da presente diretiva relativas ao direito de acesso, à informação das pessoas e à qualidade dos dados para salvaguardarem algumas finalidades dentre as acima enunciadas;

45 // Considerando que, nos casos de tratamento de dados lícito por razões de interesse público, de exercício da autoridade pública ou de interesse legítimo de uma pessoa, a pessoa em causa terá, ainda assim, o direito de, com base em razões preponderantes e legítimas relacionadas com a sua situação específica, se opor ao tratamento dos dados que lhe dizem respeito; que os Estados-membros, têm, no entanto, a possibilidade de prever disposições nacionais em contrário;

46 // Considerando que a proteção dos direitos e liberdades das pessoas em causa relativamente ao tratamento de dados pessoais exige que sejam tomadas medidas técnicas e organizacionais adequadas tanto aquando da conceção do sistema de tratamento como da realização do próprio tratamento, a fim de manter em especial a segurança e impedir assim qualquer tratamento não autorizado; que compete aos Estados-membros zelar por que os responsáveis pelo tratamento respeitem estas medidas; que estas medidas devem assegurar um nível de segurança adequado, atendendo aos conhecimentos técnicos disponíveis e ao custo da sua aplicação em função dos riscos que o tratamento implica e a natureza dos dados a proteger;

47 // Considerando que, quando uma mensagem que contém dados pessoais é transmitida através de um serviço de telecomunicações ou de correio eletrónico cujo único objetivo é a transmissão de mensagens deste tipo, será a pessoa de quem emana a mensagem, e não quem propõe o serviço de transmissão, que será em regra considerada responsável pelo tratamento dos dados pessoais contidos na mensagem; que, contudo, as pessoas que propõem esses serviços serão em regra consideradas responsáveis pelo tratamento dos dados pessoais suplementares necessários ao funcionamento do serviço;

48 // Considerando que a notificação à autoridade de controlo tem por objetivo assegurar a publicidade das finalidades e principais características do tratamento, a fim de permitir verificar a sua

conformidade com as disposições nacionais tomadas nos termos da presente diretiva;

49 // Considerando que, a fim de evitar formalidades administrativas desnecessárias, os Estados-membros podem estabelecer isenções da obrigação de notificação, ou simplificações à notificação requerida, nos casos em que o tratamento não seja suscetível de prejudicar os direitos e liberdades das pessoas em causa, desde que seja conforme com um ato adotado pelo Estado-membro que precise os seus limites; que podem igualmente ser estabelecidas isenções ou simplificações caso uma pessoa designada pelo responsável pelo tratamento se certifique de que o tratamento efetuado não é suscetível de prejudicar os direitos e liberdades das pessoas em causa; que essa pessoa encarregada da proteção de dados, empregada ou não do responsável pelo tratamento, deve exercer as suas funções com total independência;

50 // Considerando que poderá ser estabelecida a isenção ou a simplificação para tratamentos cuja única finalidade seja a manutenção de registos destinados, de acordo com o direito nacional, à informação do público e que possam ser consultados pelo público ou por qualquer pessoa que possa provar um interesse legítimo;

51 // Considerando que, no entanto, a simplificação ou a isenção da obrigação de notificação não liberam o responsável pelo tratamento de nenhuma das outras obrigações decorrentes da presente diretiva;

52 // Considerando que, neste contexto, a verificação a posteriori pelas autoridades competentes deve ser, em geral, considerada uma medida suficiente;

53 // Considerando que, no entanto, certos tratamentos podem ocasionar riscos particulares para os direitos e liberdades das pessoas em causa, em virtude da sua natureza, do seu âmbito ou da sua finalidade, como acontece, por exemplo, se esse tratamento tiver por objetivo privar as pessoas de um direito, de uma prestação ou de um contrato, ou em virtude da utilização de tecnologias novas; que compete aos Estados-membros, se assim o entenderem, precisar esses riscos na respetiva legislação;

54 // Considerando que, de todos os tratamentos efetuados em sociedade, o número dos que apresentam tais riscos particulares deverá ser muito restrito; que os Estados-membros devem estabelecer um controlo prévio à realização desses tratamentos a efetuar pela autoridade de controlo ou pelo encarregado da proteção dos dados em cooperação com essa autoridade; que, na sequência desse controlo prévio, a autoridade de controlo pode, de acordo com o direito nacional, dar um parecer ou autorizar o tratamento dos dados; que esse controlo pode igualmente ser efetuado durante os trabalhos de elaboração de uma medida legislativa do parlamento nacional ou de uma medida baseada nessa medida legislativa, a qual defina a natureza do tratamento e especifique as garantias adequadas;

55 // Considerando que, se o responsável pelo tratamento não respeitar os direitos das pessoas em causa, as legislações nacionais devem prever a possibilidade de recurso judicial; que os danos de que podem ser vítimas as pessoas em virtude de um tratamento ilegal devem ser ressarcidos pelo responsável pelo tratamento, o qual só pode ser exonerado da sua responsabilidade se provar que o facto que causou o dano lhe não é imputável, nomeadamente quando provar existir responsabilidade da pessoa em causa ou um caso de força maior; que devem ser aplicadas sanções a todas as pessoas, de direito privado ou de direito público, que não respeitem as disposições nacionais tomadas nos termos da presente diretiva;

56 // Considerando que os fluxos transfronteiras de dados pessoais são necessários ao desenvolvimento do comércio internacional; que a proteção das pessoas garantida na Comunidade pela presente diretiva não obsta às transferências de dados pessoais para países terceiros que assegurem um nível de proteção adequado; que o carácter adequado do nível de proteção oferecido por um país terceiro deve ser apreciado em função de todas as circunstâncias associadas à transferência ou a uma categoria de transferências;

57 // Considerando em contrapartida que, sempre que um país terceiro não ofereça um nível de proteção adequado, a transferência de dados pessoais para esse país deve ser proibida;

58 // Considerando que devem poder ser previstas exceções a esta proibição em certas circunstâncias, quando a pessoa em causa tiver dado o seu consentimento, quando a transferência for necessária no âmbito de um contrato ou de um processo judicial, quando a proteção de um interesse público importante assim o exigir, por exemplo nos casos de transferências internacionais de dados entre as autoridades fiscais ou aduaneiras ou entre os serviços competentes em matéria de segurança social, ou quando a transferência for feita a partir de um registo instituído por lei e destinado a consulta pelo público ou por pessoas com um interesse legítimo; que nesse caso tal transferência não deve abranger a totalidade dos dados nem as categorias de dados contidos nesse registo; que, sempre que um registo se destine a ser consultado por pessoas com um interesse legítimo, a transferência apenas deverá poder ser efetuada a pedido dessas pessoas ou caso sejam elas os seus destinatários;

59 // Considerando que podem ser tomadas medidas especiais para sanar a insuficiência de proteção num país terceiro, se o responsável pelo tratamento apresentar garantias adequadas; que, além disso, devem ser previstos processos de negociação entre a Comunidade e os países terceiros em causa;

60 // Considerando que, em todo o caso, as transferências para países terceiros só podem ser efetuadas no pleno respeito das disposições adotadas pelos Estados-membros nos termos da presente diretiva, nomeadamente do seu artigo 8º;

61 // Considerando que, no âmbito das respetivas competências, os Estados-membros e a Comissão devem incentivar as organizações sectoriais interessadas a elaborar códigos de conduta com vista a facilitar a aplicação da presente diretiva, tendo em conta as características específicas do tratamento efetuado em certos sectores e respeitando as disposições nacionais tomadas para a sua execução;

62 // Considerando que a criação nos Estados-membros de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da proteção das pessoas no que respeita ao tratamento de dados pessoais;

63 // Considerando que essas autoridades devem ser dotadas dos meios necessários para a realização das suas funções, incluindo poderes de inquérito ou de intervenção, especialmente em caso de reclamações, e poderes para intervir em processos judiciais; que essas autoridades devem ajudar a garantir a transparência do tratamento de dados efetuado no Estado-membro sob cuja jurisdição se encontram;

64 // Considerando que as autoridades dos diferentes Estados-membros deverão prestar-se mutuamente assistência no desempenho das suas funções por forma a assegurar integralmente o respeito das regras de proteção em toda a União Europeia;

65 // Considerando que deve ser criado, a nível comunitário, um grupo de trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais, o qual deve gozar de total independência no exercício das suas funções; que, atendendo à sua natureza específica, esse grupo deve aconselhar a Comissão e contribuir nomeadamente para a aplicação uniforme das normas nacionais adotadas nos termos da presente diretiva;

66 // Considerando que, no que se refere à transferência de dados para países terceiros, a aplicação da presente diretiva requer a atribuição de competências de execução à Comissão e a criação de um procedimento de acordo com as normas estabelecidas na Decisão 87/373/CEE do Conselho (1);

67 // Considerando que, em 20 de Dezembro de 1994, se chegou a acordo sobre um modus vivendi entre o Parlamento Europeu, o Conselho e a Comissão quanto às medidas de execução de atos adotados nos termos do procedimento previsto no artigo 189º B do Tratado;

68 // Considerando que os princípios enunciados na presente diretiva para a proteção dos direitos e liberdades das pessoas, nomeadamente do seu direito à vida privada, no que diz respeito ao tratamento de dados pessoais, poderão ser completados ou especificados, nomeadamente em relação a certos sectores, através de regras específicas baseadas nesses princípios;

69 // Considerando que é conveniente conceder aos Estados-membros um prazo não superior a três anos a contar da data de entrada em

vigor das medidas nacionais de transposição da presente diretiva, durante o qual essas novas disposições nacionais serão aplicadas de forma progressiva a qualquer tratamento de dados já em curso; que, para facilitar uma aplicação rentável dessas disposições, os Estados-membros poderão prever um prazo suplementar, que expirará doze anos a contar da data de adopção da presente diretiva, para assegurar a conformidade dos ficheiros, manuais existentes com determinadas disposições da diretiva; que os dados contidos nesses ficheiros, que sejam objeto de um tratamento manual efetivo durante esse período de transição suplementar, deverão ser postos em conformidade com essas disposições aquando da realização desse tratamento;

70 // Considerando que a pessoa em causa não é obrigada a dar novamente o seu consentimento para que o responsável continue a efetuar, após a entrada em vigor das disposições nacionais tomadas nos termos da presente diretiva, um tratamento de dados sensíveis necessário à execução de um contrato celebrado com base num consentimento livre e informado antes da entrada em vigor das disposições acima referidas;

71 // Considerando que a presente diretiva não obsta a que um Estado-membro regulamente as atividades de mala direta junto dos consumidores residentes no seu território, desde que a referida regulamentação não diga respeito à proteção das pessoas no que se refere ao tratamento de dados pessoais;

72 // Considerando que a presente diretiva permite tomar em consideração o princípio do direito de acesso do público aos documentos oficiais aquando da implementação dos princípios nela estabelecidos,
ADOTARAM A PRESENTE DIRETIVA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º Objeto da diretiva
1. Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à proteção assegurada por força do nº 1.

Artigo 2.º Definições
Para efeitos da presente diretiva, entende-se por:
a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

b) «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

c) «Ficheiro de dados pessoais» («ficheiro»), qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

d) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;

e) «Subcontratante», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento;

f) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados;

g) «Destinatário», a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados, independentemente de se tratar ou não de um terceiro; todavia, as autoridades suscetíveis de receberem comunicações de dados no âmbito duma missão de inquérito específica não são consideradas destinatários;

h) «Consentimento da pessoa em causa», qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Artigo 3.º Âmbito de aplicação
1. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

2. A presente diretiva não se aplica ao tratamento de dados pessoais:
- efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal,
- efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.

Artigo 4.º Direito nacional aplicável
1. Cada Estado-membro aplicará as suas disposições nacionais adotadas por força da presente diretiva ao tratamento de dados pessoais quando:
a) O tratamento for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver

estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;

b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;

c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade.

2. No caso referido na alínea c) do nº 1, o responsável pelo tratamento deve designar um representante estabelecido no território desse Estado-membro, sem prejuízo das ações que possam vir a ser intentadas contra o próprio responsável pelo tratamento.

CAPÍTULO II
CONDIÇÕES GERAIS DE LICITUDE DO TRATAMENTO DE DADOS PESSOAIS

Artigo 5.º
Os Estados-membros especificarão, dentro dos limites do disposto no presente capítulo, as condições em que é lícito o tratamento de dados pessoais.

SECÇÃO I
PRINCÍPIOS RELATIVOS À QUALIDADE DOS DADOS

Artigo 6.º
1. Os Estados-membros devem estabelecer que os dados pessoais serão:
a) Objeto de um tratamento leal e lícito;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;

c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;

d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados;

e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.

2. Incumbe ao responsável pelo tratamento assegurar a observância do disposto no nº 1.

SECÇÃO II
PRINCÍPIOS RELATIVOS
À LEGITIMIDADE DO TRATAMENTO DE DADOS

Artigo 7.º
Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se:
a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou

b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou

c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou

d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou

e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido

o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou

f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

SECÇÃO III
CATEGORIAS ESPECÍFICAS DE TRATAMENTOS

Artigo 8.º Tratamento de certas categorias específicas de dados
1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

2. O nº 1 não se aplica quando:
a) A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento, salvo se a legislação do Estado-membro estabelecer que a proibição referida no nº 1 não pode ser retirada pelo consentimento da pessoa em causa; ou

b) O tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas; ou

c) O tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento; ou

d) O tratamento for efetuado, no âmbito das suas atividades legítimas e com as garantias adequadas, por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e

de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa; ou

e) O tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.

3. O nº 1 não se aplica quando o tratamento dos dados for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços da saúde e quando o tratamento desses dados for efetuado por um profissional da saúde obrigado ao segredo profissional pelo direito nacional ou por regras estabelecidas pelos organismos nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente.

4. Sob reserva de serem prestadas as garantias adequadas, os Estados-membros poderão estabelecer, por motivos de interesse público importante, outras derrogações para além das previstas no nº 2, quer através de disposições legislativas nacionais, quer por decisão da autoridade de controlo referida no artigo 28º

5. O tratamento de dados relativos a infrações, condenações penais ou medidas de segurança só poderá ser efetuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas, sob reserva das derrogações que poderão ser concedidas pelo Estado-membro com base em disposições nacionais que prevejam garantias específicas e adequadas. Contudo, o registo completo das condenações penais só pode ser mantido sob o controlo das autoridades públicas.
Os Estados-membros podem estabelecer que o tratamento de dados relativos a sanções administrativas ou decisões cíveis fique igualmente sujeito ao controlo das autoridades públicas.

6. As derrogações ao nº 1 prevista nos nºs 4 e 5 serão notificadas à Comissão.

7. Cabe aos Estados-membros determinar as condições em que um número nacional de identificação ou qualquer outro elemento de identificação de aplicação geral poderá ser objeto de tratamento.

Artigo 9.º Tratamento de dados pessoais e liberdade de expressão
Os Estados-membros estabelecerão isenções ou derrogações ao disposto no presente capítulo e nos capítulos IV e VI para o tratamento de dados pessoais efetuado para fins exclusivamente jornalísticos ou de expressão artística ou literária, apenas na medida em que sejam necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão.

SECÇÃO IV
INFORMAÇÃO DA PESSOA EM CAUSA

Artigo 10.º Informação em caso de recolha de dados junto da pessoa em causa
Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento:
a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante;

b) Finalidades do tratamento a que os dados se destinam;

c) Outras informações, tais como:
- os destinatários ou categorias de destinatários dos dados,
- o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder,
- a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos.

Artigo 11.º Informação em caso de dados não recolhidos junto da pessoa em causa
1. Se os dados não tiverem sido recolhidos junto da pessoa em causa, os Estados-membros estabelecerão que o responsável pelo tratamento, ou o seu representante, deve fornecer à pessoa em causa, no momento em que os dados forem registados ou, se estiver prevista a comunicação de dados a terceiros, o mais tardar aquando da primeira comunicação desses dados, pelo menos as seguintes informações, salvo se a referida pessoa já delas tiver conhecimento:

a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante;

b) Finalidades do tratamento;

c) Outras informações, tais como:
- as categorias de dados envolvidos,
- os destinatários ou categorias de destinatários dos dados,
- a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos.

2. O nº 1 não se aplica quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação da pessoa em causa se revelar impossível ou implicar esforços desproporcionados ou quando a lei dispuser expressamente o registo dos dados ou a sua divulgação. Nestes casos, os Estados-membros estabelecerão as garantias adequadas.

SECÇÃO V
DIREITO DE ACESSO DA PESSOA EM CAUSA AOS DADOS

Artigo 12.º Direito de acesso
Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento:
a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos:
- a confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados,
- a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados,
- o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º;

b) Consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente diretiva, nomeadamente devido ao carácter incompleto ou inexato desses dados;

c) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer retificação, apagamento ou bloqueio efetuado nos termos da alínea b), salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado.

SECÇÃO VI
DERROGAÇÕES E RESTRIÇÕES

Artigo 13.º Derrogações e restrições

1. Os Estados-membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos no nº 1 do artigo 6º, no artigo 10º, no nº 1 do artigo 11º e nos artigos 12º e 21º, sempre que tal restrição constitua uma medida necessária à proteção:
a) Da segurança do Estado;

b) Da defesa;

c) Da segurança pública;

d) Da prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas;

e) De um interesse económico ou financeiro importante de um Estado-membro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal;

f) De missões de controlo, de inspeção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d) e e);

g) De pessoa em causa ou dos direitos e liberdades de outrem.

2. Sob reserva de garantias jurídicas adequadas, nomeadamente a de que os dados não serão utilizados para tomar medidas ou decisões em relação a pessoas determinadas, os Estados-membros poderão

restringir através de uma medida legislativa os direitos referidos no artigo 12º nos casos em que manifestamente não exista qualquer perigo de violação do direito à vida privada da pessoa em causa e os dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas.

SECÇÃO VII
DIREITO DE OPOSIÇÃO DA PESSOA EM CAUSA

Artigo 14.º Direito de oposição da pessoa em causa
Os Estados-membros reconhecerão à pessoa em causa o direito de:
a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efetuado pelo responsável deixa de poder incidir sobre esses dados;

b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de mala direta; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de mala direta ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.
Os Estados-membros tomarão as medidas necessárias para garantir que as pessoas em causa tenham conhecimento do direito referido no primeiro parágrafo da alínea b).

Artigo 15.º Decisões individuais automatizadas
1. Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento.

2. Os Estados-membros estabelecerão, sob reserva das restantes disposições da presente diretiva, que uma pessoa pode ficar sujeita a uma decisão do tipo referido no nº 1 se a mesma:
a) For tomada no âmbito da celebração ou da execução de um contrato, na condição de o pedido de celebração ou execução do contrato apresentado pela pessoa em causa ter sido satisfeito, ou de existirem medidas adequadas, tais como a possibilidade de apresentar o seu ponto de vista, que garantam a defesa dos seus interesses legítimos; ou

b) For autorizada por uma lei que estabeleça medidas que garantam a defesa dos interesses legítimos da pessoa em causa.

SECÇÃO VIII
CONFIDENCIALIDADE E SEGURANÇA DO TRATAMENTO

Artigo 16.º Confidencialidade do tratamento
Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais.

Artigo 17.º Segurança do tratamento
1. Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.
Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

2. Os Estados-membros estabelecerão que o responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efetuar e deverá zelar pelo cumprimento dessas medidas.

3. A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou ato jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que:
- o subcontratante apenas atuará mediante instruções do responsável pelo tratamento,
- as obrigações referidas no nº 1, tal como definidas pela legislação do Estado-membro onde o subcontratante está estabelecido, incumbem igualmente a este último.

4. Para efeitos de conservação de provas, os elementos do contrato ou do ato jurídico relativos à proteção dos dados, bem como as exigências relativas às medidas referidas no nº 1, deverão ficar consignados por escrito ou sob forma equivalente.

SECÇÃO IX
NOTIFICAÇÃO

Artigo 18.º Obrigação de notificação à autoridade de controlo
1. Os Estados-membros estabelecerão que o responsável pelo tratamento ou, eventualmente, o seu representante deve notificar a autoridade de controlo referida no artigo 28º antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados à prossecução de uma ou mais finalidades interligadas.

2. Os Estados-membros apenas poderão estabelecer a simplificação ou a isenção da notificação nos seguintes casos e condições:
- se, para as categorias de tratamentos que, atendendo aos dados a tratar, não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa, especificarem as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de pessoas em causa, os destinatários ou categorias de destinatários a quem serão comunicados os dados e o período de conservação dos dados; e/ou
- se o responsável pelo tratamento nomear, nos termos do direito nacional a que está sujeito, um encarregado da proteção dos dados pessoais, responsável nomeadamente por
- garantir, de modo independente, a aplicação, a nível interno, das disposições nacionais tomadas nos termos da presente diretiva,
- manter um registo dos tratamentos efetuados pelo responsável do

tratamento, contendo as informações referidas no nº 2 do artigo 21º, assegurando assim que os tratamentos não são suscetíveis de prejudicar os direitos e liberdades das pessoas em causa.

3. Os Estados-membros poderão estabelecer que o nº 1 não se aplica a tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem à informação do público e se encontrem abertos à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo.

4. Os Estados-membros podem isentar da obrigação de notificação os tratamentos de dados referidos no nº 2, alínea d), do artigo 8º, ou prever uma simplificação dessa notificação.

5. Os Estados-membros podem determinar que todos ou alguns dos tratamentos não automatizados de dados pessoais sejam notificados, eventualmente de forma simplificada.

Artigo 19.º Conteúdo de notificação

1. Os Estados-membros especificarão as informações que devem constar da notificação. Essas informações devem incluir, pelo menos:

a) O nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante;

b) A ou as finalidades do tratamento;

c) Uma descrição da ou das categorias de pessoas em causa e dos dados ou categorias de dados que lhes respeitem;

d) Os destinatários ou categorias de destinatários a quem os dados poderão ser comunicados;

e) As transferências de dados previstas para países terceiros;

f) Uma descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação do artigo 17º

2. Os Estados-membros especificarão os procedimentos de notificação à autoridade de controlo das alterações que afetem as informações referidas no nº 1.

Artigo 20.º Controlo prévio

1. Os Estados-membros especificarão os tratamentos que possam representar riscos específicos para os direitos e liberdades das pessoas em causa e zelarão por que sejam controlados antes da sua aplicação.

2. Esse controlo prévio será efetuado pela autoridade de controlo referida no artigo 28º após receção de uma notificação do responsável pelo tratamento ou pelo encarregado da proteção de dados que, em caso de dúvida, deverá consultar a autoridade de controlo.

3. Os Estados-membros poderão igualmente efetuar este controlo durante os trabalhos de preparação de uma medida do parlamento nacional ou de uma medida baseada nessa medida legislativa, a qual defina a natureza do tratamento e estabeleça as garantias adequadas.

Artigo 21.º Publicidade dos tratamentos

1. Os Estados-membros tomarão as medidas necessárias para assegurar a publicidade dos tratamentos.

2. Os Estados-membros estabelecerão que a autoridade de controlo referida no artigo 28º manterá um registo dos tratamentos notificados por força do artigo 18º.

Esse registo deverá conter, pelo menos, as informações enumeradas no nº 1, alíneas a) a e), do artigo 19º.
O registo poderá ser consultado por qualquer pessoa.

3. Os Estado-membros estabelecerão que, no que respeita aos tratamentos não sujeitos a notificação, o responsável pelo tratamento, ou outra entidade designada pelos Estados-membros, comunicará de forma adequada, a qualquer pessoa que o solicite, pelo menos as informações referidas no nº 1, alíneas a) a e), do artigo 19º

Os Estados-membros poderão estabelecer que a presente disposição não se aplica a tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares,

se destinem à informação do público e se encontrem abertos à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo.

CAPÍTULO III
RECURSOS JUDICIAIS, RESPONSABILIDADE E SANÇÕES

Artigo 22.º Recursos
Sem prejuízo de quaisquer garantias graciosas, nomeadamente por parte da autoridade de controlo referida no artigo 28º, previamente a um recurso contencioso, os Estados-membros estabelecerão que qualquer pessoa poderá recorrer judicialmente em caso de violação dos direitos garantidos pelas disposições nacionais aplicáveis ao tratamento em questão.

Artigo 23.º Responsabilidade
1. Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato incompatível com as disposições nacionais de execução da presente diretiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido.

2. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

Artigo 24.º Sanções
Os Estados-membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente diretiva a determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adotadas nos termos da presente diretiva.

CAPÍTULO IV
TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

Artigo 25.º Princípios
1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a

ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um nível de proteção adequado.

2. A adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país.

3. Os Estados-membros e a Comissão informar-se-ão mutuamente dos casos em que consideram que um país terceiro não assegura um nível de proteção adequado na aceção do nº 2.

4. Sempre que a Comissão verificar, nos termos do procedimento previsto no nº 2 do artigo 31º, que um país terceiro não assegura um nível de proteção adequado na aceção do nº 2 do presente artigo, os Estados-membros tomarão as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa.

5. Em momento oportuno, a Comissão encetará negociações com vista a obviar à situação resultante da constatação feita em aplicação do nº 4.

6. A Comissão pode constatar, nos termos do procedimento previsto no nº 2 do artigo 31º, que um país terceiro assegura um nível de proteção adequado na aceção do nº 2 do presente artigo em virtude da sua legislação interna ou dos seus compromissos internacionais, subscritos nomeadamente na sequência das negociações referidas no nº 5, com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

Os Estados-membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

Artigo 26.º Derrogações

1. Em derrogação ao disposto no artigo 25º e sob reserva de disposições em contrário do seu direito nacional em casos específicos, os Estados-membros estabelecerão que a transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado na aceção do nº 2 do artigo 25º poderá ter lugar desde que:

a) A pessoa em causa tenha dado de forma inequívoca o seu consentimento à transferência; ou

b) A transferência seja necessária para a execução de um contrato entre a pessoa em causa e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou

c) A transferência seja necessária à execução ou celebração de um contrato celebrado ou a celebrar, no interesse da pessoa em causa, entre o responsável pelo tratamento e um terceiro; ou

d) A transferência seja necessária ou legalmente exigida para a proteção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou

e) A transferência seja necessária para proteger os interesses vitais da pessoa em causa; ou

f) A transferência seja realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2. Sem prejuízo do nº 1, um Estado-membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro que não assegura um nível de proteção adequado na aceção do nº 2 do artigo 25º, desde que o responsável pelo tratamento apresente garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respetivos direitos; essas garantias podem, designadamente, resultar de cláusulas contratuais adequadas.

3. O Estado-membro informará a Comissão e os restantes Estados-membros das autorizações que conceder nos termos do nº 2.
Em caso de oposição, por um Estado-membro ou pela Comissão devidamente justificada no que se refere à proteção da privacidade e dos direitos e liberdades fundamentais das pessoas, a Comissão adotará as medidas adequadas, nos termos do procedimento previsto no nº 2 do artigo 31º

Os Estados-membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

4. Sempre que a Comissão decidir, nos termos do procedimento previsto no nº 2 do artigo 31º, que certas cláusulas contratuais-tipo oferecem as garantias suficientes referidas no nº 2, os Estados-membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

CAPÍTULO V
CÓDIGOS DE CONDUTA

Artigo 27.º
1. Os Estados-membros e a Comissão promoverão a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes sectores, para a boa execução das disposições nacionais tomadas pelos Estados-membros nos termos da presente diretiva.

2. Os Estados-membros estabelecerão que as associações profissionais e as outras organizações representativas de outras categorias de responsáveis pelo tratamento que tenham elaborado projetos de códigos nacionais ou que tencionem alterar ou prorrogar códigos nacionais existentes, podem submetê-los à apreciação das autoridades nacionais.

Os Estados-membros estabelecerão que essas autoridades se certificarão, nomeadamente, da conformidade dos projetos que lhe são apresentados com as disposições nacionais tomadas nos termos da presente diretiva. Se o considerarem oportuno, as autoridades solicitarão a opinião das pessoas em causa ou dos seus representantes.

3. Os projetos de códigos comunitários, assim como as alterações ou prorrogações de códigos comunitários existentes, poderão ser submetidos

ao grupo referido no artigo 29º O grupo pronunciar-se-á, nomeadamente, quanto à conformidade dos projetos submetidos à sua apreciação com as disposições nacionais adotadas em aplicação da presente diretiva. Se o considerar oportuno, solicitará a opinião das pessoas em causa ou dos seus representantes. A Comissão pode garantir uma publicidade adequada dos códigos aprovados pelo grupo.

CAPÍTULO VI
AUTORIDADE DE CONTROLO E GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Artigo 28.º Autoridade de controlo

1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-membros nos termos da presente diretiva.

Essas autoridades exercerão com total independência as funções que lhes forem atribuídas.

2. Cada Estado-membro estabelecerá que as autoridades de controlo serão consultadas aquando da elaboração de medidas regulamentares ou administrativas relativas à proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais.

3. Cada autoridade do controlo disporá, nomeadamente:
- de poderes de inquérito, tais como o poder de aceder aos dados objeto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controlo,
- de poderes efetivos de intervenção, tais como, por exemplo, o de emitir pareceres previamente à execução adequada desses pareceres, o de ordenar o bloqueio, o apagamento ou a destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentos nacionais ou para outras instituições políticas,
- do poder de intervir em processos judiciais no caso de violação das disposições nacionais adotadas nos termos da presente diretiva ou de

levar essas infrações ao conhecimento das autoridades judiciais.
As decisões da autoridade de controlo que lesem interesses são passíveis de recurso jurisdicional.

4. Qualquer pessoa ou associação que a represente pode apresentar à autoridade de controlo um pedido para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais. A pessoa em causa será informada do seguimento dado ao seu pedido.
Em particular, qualquer pessoa pode apresentar à autoridade de controlo um pedido de verificação da licitude de qualquer tratamento de dados, sempre que sejam aplicáveis as disposições nacionais adotadas por força do artigo 13º O requerente será pelo menos informado da realização da verificação.

5. Cada autoridade de controlo elaborará periodicamente um relatório sobre a sua atividade. O relatório será publicado.

6. Cada autoridade de controlo é competente, independentemente do direito nacional aplicável ao tratamento em causa, para o exercício no território do seu Estado-membro dos poderes que lhe foram atribuídos em conformidade com o nº 3. Cada autoridade de controlo pode ser solicitada a exercer os seus poderes por uma autoridade de outro Estado-membro.

As autoridades de controlo cooperarão entre si na medida do necessário ao desempenho das suas funções, em especial através do intercâmbio de quaisquer informações úteis.

7. Os Estados-membros determinarão que os membros e agentes das autoridades de controlo fiquem sujeitos, mesmo após a cessação das suas atividades, à obrigação de segredo profissional em relação às informações confidenciais a que tenham acesso.

Artigo 29.º Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais
1. É criado um Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, a seguir designado «grupo».
O grupo tem carácter consultivo e é independente.

2. O grupo é composto por um representante da autoridade ou autoridades de controlo designadas por cada Estado-membro, por um representante da autoridade ou autoridades criadas para as instituições e organismos comunitários, bem como por um representante da Comissão.

Cada membro do grupo será designado pela instituição, autoridade ou autoridades que representa. Sempre que um Estado-membro tiver designado várias autoridades de controlo, estas nomearão um representante comum. O mesmo acontece em relação às autoridades criadas para as instituições e organismos comunitários.

3. O grupo tomará as suas decisões por maioria simples dos representantes das autoridades de controlo.

4. O grupo elegerá o seu presidente. O mandato do presidente tem uma duração de dois anos e é renovável.

5. O secretariado do grupo será assegurado pela Comissão.

6. O grupo elaborará o seu regulamento interno.

7. O grupo analisará as questões inscritas na ordem de trabalhos pelo seu presidente, que por iniciativa deste, quer a pedido de um representante das autoridades de controlo, quer ainda a pedido da Comissão.

Artigo 30.º
1. O grupo tem por atribuições:
a) Analisar quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da presente diretiva, com vista a contribuir para a sua aplicação uniforme;

b) Dar parecer à Comissão sobre o nível de proteção na Comunidade e nos países terceiros;

c) Aconselhar a Comissão sobre quaisquer projetos de alteração da presente diretiva ou sobre quaisquer projetos de medidas adicionais ou específicas a tomar para proteger os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como sobre quaisquer outros projetos de medidas comunitárias com

incidência sobre esses direitos e liberdades;

d) Dar parecer sobre os códigos de conduta elaborados a nível comunitário.

2. Se o grupo verificar que surgem divergências suscetíveis de prejudicar a equivalência da proteção das pessoas no que diz respeito ao tratamento de dados pessoais na Comunidade entre a legislação ou a prática dos Estados-membros, informará desse facto a Comissão.

3. O grupo pode, por sua própria iniciativa, formular recomendações sobre quaisquer questões relativas à proteção das pessoas no que diz respeito ao tratamento de dados pessoais na Comunidade.

4. Os pareceres e recomendações do grupo serão transmitidos à Comissão e ao comité referido no artigo 31º.

5. A Comissão informará o grupo do seguimento que deu aos seus pareceres e recomendações. Para o efeito, elaborará um relatório que será igualmente enviado ao Parlamento Europeu e ao Conselho. O relatório será publicado.

6. O grupo elaborará um relatório anual sobre a situação da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais na Comunidade e nos países terceiros, que será comunicado à Comissão, ao Parlamento Europeu e ao Conselho. O relatório será publicado.

CAPÍTULO VII
MEDIDAS DE EXECUÇÃO COMUNITÁRIAS

Artigo 31.º Comitologia
1. A Comissão será assistida por um comité composto por representantes dos Estados-membros e presidido pelo representante da Comissão.

2. O representante da Comissão submeterá à apreciação do comité um projeto das medidas a tomar. O comité emitirá o seu parecer sobre esse projeto num prazo que o presidente pode fixar em função da urgência da questão em causa.

O parecer será emitido por maioria, nos termos previstos no nº 2 do artigo 148º do Tratado. Nas votações no comité, os votos dos representantes dos Estados-membros estão sujeitos à ponderação definida no artigo atrás referido. O presidente não participa na votação.

A Comissão adotará medidas que são imediatamente aplicáveis. Todavia, se não forem conformes com o parecer emitido pelo comité, essas medidas serão imediatamente comunicadas pela Comissão ao Conselho. Nesse caso:
- a Comissão diferirá a aplicação das medidas que aprovou por um prazo de três meses a contar da data da comunicação,
- o Conselho, deliberando por maioria qualificada, pode tomar uma decisão diferente no prazo previsto no travessão anterior.

DISPOSIÇÕES FINAIS

Artigo 32.º
1. Os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva o mais tardar três anos a contar da data da sua adoção. Quando os Estados-membros adotarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência na publicação oficial. As modalidades dessa referência serão adotadas pelos Estados-membros.

2. Os Estados-membros assegurarão que os tratamentos já em curso à data da entrada em vigor das disposições nacionais tomadas nos termos da presente diretiva cumprirão essas disposições o mais tardar três anos a contar da referida data.

Em derrogação ao parágrafo anterior, os Estados-membros poderão estabelecer que o tratamento de dados já existente em ficheiros manuais à data de entrada em vigor das disposições nacionais tomadas nos termos da presente diretiva cumprirá o disposto nos artigos 6º, 7º e 8º no prazo de doze anos a contar da data de adoção da presente diretiva. Os Estados-membros possibilitarão, no entanto, à pessoa em causa obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a retificação, o apagamento ou o bloqueio dos dados incompletos, inexatos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.

3. Em derrogação ao nº 2, os Estados-membros poderão estabelecer que, sob reserva das garantias adequadas, os dados conservados unicamente com finalidades de investigação histórica não terão que cumprir os artigos 6º, 7º e 8º da presente diretiva.

4. Os Estados-membros comunicarão à Comissão o texto das disposições de direito interno que adotem no domínio regido pela presente diretiva.

Artigo 33.º
A Comissão apresentará periodicamente ao Parlamento Europeu e ao Conselho, e pela primeira vez o mais tardar três anos após a data referida no nº 1 do artigo 32º, um relatório sobre a aplicação da presente diretiva, eventualmente acompanhado de propostas de alteração adequadas. O relatório será publicado.

A Comissão analisará, nomeadamente, a aplicação da presente diretiva ao tratamento de dados de som e de imagem relativos às pessoas singulares e apresentará as propostas adequadas que se revelem necessárias, tendo em conta o desenvolvimento das tecnologias da informação, e à luz da situação quanto aos trabalhos sobre a sociedade de informação.

Artigo 34.º
Os Estados-membros são os destinatários da presente diretiva.

Feito no Luxemburgo, em 24 de Outubro de 1995.
Pelo Parlamento Europeu
O Presidente
Pelo Conselho
O Presidente

3. Constituição da República Portuguesa
(Artigos 26 e 35.º)

(…)

Artigo 26.º Outros direitos pessoais
1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação.

2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.

3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica.

4. A privação da cidadania e as restrições à capacidade civil só podem efetuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos.

(…)

Artigo 35.º Utilização da informática
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias

de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

(…)

4. Tratado sobre o funcionamento da União Europeia
(Artigo 16.º)

(…)

Artigo 16.º

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia.

(…)

5. Carta dos Direitos Fundamentais da União Europeia (Artigos 7.º, 8.º e 11.º)

(…)

Artigo 7.º Respeito pela vida privada e familiar
Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.º Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

(…)

Artigo 11.º Liberdade de expressão e de informação
1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras.

2. São respeitados a liberdade e o pluralismo dos meios de comunicação social.

(…)

6. Código Civil
(Artigos 70.º a 81.º)

(...)

SECÇÃO II
DIREITOS DE PERSONALIDADE

Artigo 70.º Tutela geral da personalidade
1. A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.

2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida.

Artigo 71.º Ofensa a pessoas já falecidas
1. Os direitos de personalidade gozam igualmente de proteção depois da morte do respetivo titular.

2. Tem legitimidade, neste caso, para requerer as providências previstas no n.º 2 do artigo anterior o cônjuge sobrevivo ou qualquer descendente, ascendente, irmão, sobrinho ou herdeiro do falecido.

3. Se a ilicitude da ofensa resultar da falta de consentimento, só as pessoas que o deveriam prestar têm legitimidade, conjunta ou separadamente, para requerer as providências a que o número anterior se refere.

Artigo 72.º Direito ao nome
1. Toda a pessoa tem direito a usar o seu nome, completo ou abreviado, e a opor-se a que outrem o use ilicitamente para sua identificação ou outros fins.

2. O titular do nome não pode, todavia, especialmente no exercício de uma atividade profissional, usá-lo de modo a prejudicar os interesses de quem tiver nome total ou parcialmente idêntico; nestes casos, o tribunal decretará as providências que, segundo juízos de equidade, melhor conciliem os interesses em conflito.

Artigo 73.º Legitimidade
As ações relativas à defesa do nome podem ser exercidas não só pelo respetivo titular, como, depois da morte dele pelas pessoas referidas no n.º 2 do artigo 71.º

Artigo 74.º Pseudónimo
O pseudónimo, quando tenha notoriedade, goza da proteção conferida ao próprio nome.

Artigo 75.º Cartas-missivas confidenciais
1. O destinatário de carta-missiva de natureza confidencial deve guardar reserva sobre o seu conteúdo, não lhe sendo lícito aproveitar os elementos de informação que ela tenha levado ao seu conhecimento.

2. Morto o destinatário, pode a restituição da carta confidencial ser ordenada pelo tribunal, a requerimento do autor dela ou, se este já tiver falecido, das pessoas indicadas no n.º 2 do artigo 71.º; pode também ser ordenada a destruição da carta, o seu depósito em mão de pessoa idónea ou qualquer outra medida apropriada.

Artigo 76.º Publicação de cartas confidenciais
1. As cartas-missivas confidenciais só podem ser publicadas com o consentimento do seu autor ou com o suprimento judicial desse consentimento; mas não há lugar ao suprimento quando se trate de utilizar as cartas como documento literário, histórico ou biográfico.

2. Depois da morte do autor, a autorização compete às pessoas designadas no n.º 2 do artigo 71.º, segundo a ordem nele indicada.

Artigo 77.º Memórias familiares e outros escritos confidenciais
O disposto no artigo anterior é aplicável, com às necessárias adaptações, as memórias familiares e pessoais e a outros escritos que tenham carácter confidencial ou se refiram à intimidade da vida privada.

Artigo 78.º Cartas-missivas não confidenciais
O destinatário de carta não confidencial só pode usar dela em termos que não contrariem a expectativa do autor.

Artigo 79.º Direito à imagem
1. O retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela; depois da morte da pessoa retratada, a autorização compete às pessoas designadas no n.º 2 do artigo 71.º, segundo a ordem nele indicada.

2. Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente.

3. O retrato não pode, porém, ser reproduzido, exposto ou lançado no comércio, se do facto resultar prejuízo para a honra, reputação ou simples decoro da pessoa retratada.

Artigo 80.º Direito à reserva sobre a intimidade da vida privada
1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.

2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas.

Artigo 81.º Limitação voluntária dos direitos de personalidade
1. Toda a limitação voluntária ao exercício dos direitos de personalidade é nula, se for contrária aos princípios da ordem pública.

2. A limitação voluntária, quando legal, é sempre revogável, ainda que com obrigação de indemnizar os prejuízos causados às legítimas expectativas da outra parte.

(...)

7. Código do Trabalho (Artigos 14.º a 22.º, 32.º, 97.º a 99.º, 106.º 107.º, 171.º, 202.º, 332.º, 548.º a 566.º)

LIVRO I
PARTE GERAL

(...)

TITULO II
CONTRATO DE TRABALHO

CAPÍTULO I
DISPOSIÇÕES GERAIS

SECÇÃO I
CONTRATO DE TRABALHO

(...)

SECÇÃO II
SUJEITOS

(...)

SUBSECÇÃO II
DIREITOS DE PERSONALIDADE

Artigo 14.º Liberdade de expressão e de opinião
É reconhecida no âmbito da empresa a liberdade de expressão e de divulgação do pensamento e opinião, com respeito dos direitos de personalidade do trabalhador e empregador, incluindo as pessoas singulares que o representam, e do normal funcionamento da empresa.

Artigo 15.º Integridade Física e Moral
O empregador, incluindo as pessoas singulares que o representam, e o trabalhador gozam do direito à respetiva integridade física e moral.

Artigo 16.º Reserva da intimidade da vida privada
1. O empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada.

2. O direito à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas.

Artigo 17.º Proteção de dados pessoais
1. O empregador não pode exigir a candidato a emprego ou a trabalhador que preste informações relativas:
a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação;

b) À sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação.

2. As informações previstas na alínea b) do número anterior são prestadas a médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a atividade.

3. O candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respetivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua retificação e atualização.

4. Os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à proteção de dados pessoais.

5. Constitui contraordenação muito grave a violação do disposto nos n.ºs 1 ou 2.

Artigo 18.º Dados biométricos
1. O empregador só pode tratar dados biométricos do trabalhador após notificação à Comissão Nacional de Protecção de Dados.

2. O tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir.

3. Os dados biométricos são conservados durante o período necessário

para a prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho.

4. A notificação a que se refere o n.º 1 deve ser acompanhada de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer.

5. Constitui contraordenação grave a violação do disposto no n.º 3.

Artigo 19.º Testes e exames médicos
1. Para além das situações previstas em legislação relativa a segurança e saúde no trabalho, o empregador não pode, para efeitos de admissão ou permanência no emprego, exigir a candidato a emprego ou a trabalhador a realização ou apresentação de testes ou exames médicos, de qualquer natureza, para comprovação das condições físicas ou psíquicas, salvo quando estes tenham por finalidade a proteção e segurança do trabalhador ou de terceiros, ou quando particulares exigências inerentes à atividade o justifiquem, devendo em qualquer caso ser fornecida por escrito ao candidato a emprego ou trabalhador a respetiva fundamentação.

2. O empregador não pode, em circunstância alguma, exigir a candidata a emprego ou a trabalhadora a realização ou apresentação de testes ou exames de gravidez.

3. O médico responsável pelos testes e exames médicos só pode comunicar ao empregador se o trabalhador está ou não apto para desempenhar a atividade.

4. Constitui contraordenação muito grave a violação do disposto nos n.ºs 1 ou 2.

Artigo 20.º Meios de vigilância a distância
1. O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador.

2. A utilização de equipamento referido no número anterior é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem.

3. Nos casos previstos no número anterior, o empregador informa o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo.

4. Constitui contraordenação muito grave a violação do disposto no n.º 1 e constitui contraordenação leve a violação do disposto no n.º 3.

Artigo 21.º Utilização de meios de vigilância a distância
1. A utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Protecção de Dados.

2. A autorização só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objetivos a atingir.

3. Os dados pessoais recolhidos através dos meios de vigilância a distância são conservados durante o período necessário para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho.

4. O pedido de autorização a que se refere o n.º 1 deve ser acompanhado de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer.

5. Constitui contraordenação grave a violação do disposto no n.º 3

Artigo 22.º Confidencialidade de mensagens e de acesso a informação
1. O trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio eletrónico.

2. O disposto no número anterior não prejudica o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico.

(…)

SUBSECÇÃO III
DIVISÃO III
IGUALDADE E NÃO DISCRIMINAÇÃO EM FUNÇÃO DO SEXO

(…)

Artigo 32.º Registo de processos de recrutamento
1. Todas as entidades devem manter durante cinco anos o registo dos processos de recrutamento efetuados, devendo constar do mesmo, com desagregação por sexo, os seguintes elementos:
a) Convites para o preenchimento de lugares;

b) Anúncios de oferta de emprego;

c) Número de candidaturas para apreciação curricular;

d) Número de candidatos presentes em entrevistas de pré-seleção;

e) Número de candidatos aguardando ingresso;

f) Resultados de testes ou provas de admissão ou seleção;

g) Balanços sociais relativos a dados, que permitam analisar a existência de eventual discriminação de pessoas de um dos sexos no acesso ao emprego, formação e promoção profissionais e condições de trabalho.

2. Constitui contraordenação leve a violação do disposto neste artigo .

(…)

SUBSECÇÃO IX
O EMPREGADOR E A EMPRESA

Artigo 97.º Poder de direção
Compete ao empregador estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem.

Artigo 98.º Poder disciplinar
O empregador tem poder disciplinar sobre o trabalhador ao seu serviço, enquanto vigorar o contrato de trabalho.

Artigo 99.º Regulamento interno de empresa
1. O empregador pode elaborar regulamento interno de empresa sobre organização e disciplina do trabalho.

2. Na elaboração do regulamento interno de empresa é ouvida a comissão de trabalhadores ou, na sua falta, as comissões intersindicais, as comissões sindicais ou os delegados sindicais.

3. O regulamento interno produz efeitos após a publicitação do respetivo conteúdo, designadamente através de afixação na sede da empresa e nos locais de trabalho, de modo a possibilitar o seu pleno conhecimento, a todo o tempo, pelos trabalhadores.

4. A elaboração de regulamento interno de empresa sobre determinadas matérias pode ser tornada obrigatória por instrumento de regulamentação coletiva de trabalho negocial.

5. Constitui contraordenação grave a violação do disposto nos n.ºs 2 e 3.

(…)

SECÇÃO III
FORMAÇÃO DO CONTRATO

(…)

SUBSECÇÃO IV
INFORMAÇÃO SOBRE ASPETOS RELEVANTES NA PRESTAÇÃO DE TRABALHO

Artigo 106.º Dever de informação
1. O empregador deve informar o trabalhador sobre aspetos relevantes do contrato de trabalho.

2. O trabalhador deve informar o empregador sobre aspetos relevantes para a prestação da atividade laboral.

3. O empregador deve prestar ao trabalhador, pelo menos, as seguintes informações:
a) A respetiva identificação, nomeadamente, sendo sociedade, a existência de uma relação de coligação societária, de participações recíprocas, de domínio ou de grupo, bem como a sede ou domicílio;

b) O local de trabalho ou, não havendo um fixo ou predominante, a indicação de que o trabalho é prestado em várias localizações;

c) A categoria do trabalhador ou a descrição sumária das funções correspondentes;

d) A data de celebração do contrato e a do início dos seus efeitos;

e) A duração previsível do contrato, se este for celebrado a termo;

f) A duração das férias ou o critério para a sua determinação;

g) Os prazos de aviso prévio a observar pelo empregador e pelo trabalhador para a cessação do contrato, ou o critério para a sua determinação;

h) O valor e a periodicidade da retribuição;

i) O período normal de trabalho diário e semanal, especificando os casos em que é definido em termos médios;

j) O número da apólice de seguro de acidentes de trabalho e a identificação da entidade seguradora;

l) O instrumento de regulamentação coletiva de trabalho aplicável, se houver.

m) A identificação do fundo de compensação do trabalho ou de mecanismo equivalente, bem como do fundo de garantia de compensação do trabalho, previstos em legislação específica.

4. A informação sobre os elementos referidos nas alíneas f) a i) do número anterior pode ser substituída pela referência às disposições pertinentes da lei, do instrumento de regulamentação coletiva de trabalho aplicável ou do regulamento interno de empresa.

5. Constitui contraordenação grave a violação do disposto em qualquer alínea do n.º 3.

Artigo 107.º Meios de informação
1. A informação prevista no artigo anterior deve ser prestada por escrito, podendo constar de um ou de vários documentos, assinados pelo empregador.

2. Quando a informação seja prestada através de mais de um documento, um deles deve conter os elementos referidos nas alíneas a) a d), h) e i) do n.º 3 do artigo anterior.

3. O dever previsto no n.º 1 do artigo anterior considera-se cumprido quando a informação em causa conste de contrato de trabalho reduzido a escrito ou de contrato-promessa de contrato de trabalho.

4. Os documentos referidos nos n.ºs 1 e 2 devem ser entregues ao trabalhador nos 60 dias subsequentes ao início da execução do contrato ou, se este cessar antes deste prazo, até ao respetivo termo.

5. Constitui contraordenação grave a violação do disposto nos n.ºs 1, 2 ou 4.

(...)

SECÇÃO IX
MODALIDADES DE CONTRATO DE TRABALHO

(...)

SUBSECÇÃO V
TELETRABALHO

(...)

Artigo 169.º Igualdade de tratamento de trabalhador em regime de teletrabalho
1.O trabalhador em regime de teletrabalho tem os mesmos direitos e deveres dos demais trabalhadores, nomeadamente no que se refere a formação e promoção ou carreira profissionais, limites do período normal de trabalho e outras condições de trabalho, segurança e saúde no trabalho e reparação de danos emergentes de acidente de trabalho ou doença profissional.

2. No âmbito da formação profissional, o empregador deve proporcionar ao trabalhador, em caso de necessidade, formação adequada sobre a utilização de tecnologias de informação e de comunicação inerentes ao exercício da respetiva atividade.

3. O empregador deve evitar o isolamento do trabalhador, nomeadamente através de contactos regulares com a empresa e os demais trabalhadores.

Artigo 170.º Privacidade de trabalhador em regime de teletrabalho
1. O empregador deve respeitar a privacidade do trabalhador e os tempos de descanso e de repouso da família deste, bem como proporcionar-lhe boas condições de trabalho, tanto do ponto de vista físico como psíquico.

2. Sempre que o teletrabalho seja realizado no domicílio do trabalhador, a visita ao local de trabalho só deve ter por objeto o controlo da atividade laboral, bem como dos instrumentos de trabalho e apenas pode ser efetuada entre as 9 e as 19 horas, com a assistência do trabalhador ou de pessoa por ele designada.

3. Constitui contraordenação grave a violação do disposto neste artigo.

Artigo 171.º Participação e representação coletivas de trabalhador em regime de teletrabalho
1. O trabalhador em regime de teletrabalho integra o número de trabalhadores da empresa para todos os efeitos relativos a estruturas de representação coletiva, podendo candidatar-se a essas estruturas.

2. O trabalhador pode utilizar as tecnologias de informação e de comunicação afetas à prestação de trabalho para participar em reunião promovida no local de trabalho por estrutura de representação coletiva dos trabalhadores.

3. Qualquer estrutura de representação coletiva dos trabalhadores pode utilizar as tecnologias referidas no número anterior para, no exercício da sua atividade, comunicar com o trabalhador em regime de teletrabalho, nomeadamente divulgando informações a que se refere o n.º 1 do artigo 465.º

4. Constitui contraordenação grave a violação do disposto nos n.ºs 2 ou 3.

(...)

CAPÍTULO II
PRESTAÇÃO DO TRABALHO

(...)

SECÇÃO II
DURAÇÃO E ORGANIZAÇÃO DO TEMPO DE TRABALHO

SUBSECÇÃO I
NOÇÕES E PRINCÍPIOS GERAIS SOBRE DURAÇÃO E ORGANIZAÇÃO DO TEMPO DE TRABALHO

Artigo 202.º Registo de tempos de trabalho

1. O empregador deve manter o registo dos tempos de trabalho, incluindo dos trabalhadores que estão isentos de horário de trabalho, em local acessível e por forma que permita a sua consulta imediata.

2. O registo deve conter a indicação das horas de início e de termo do tempo de trabalho, bem como das interrupções ou intervalos que nele não se compreendam, por forma a permitir apurar o número de horas de trabalho prestadas por trabalhador, por dia e por semana, bem como as prestadas em situação referida na alínea b) do n.º 1 do artigo 257.º

3. O empregador deve assegurar que o trabalhador que preste trabalho no exterior da empresa vise o registo imediatamente após o seu regresso à empresa, ou envie o mesmo devidamente visado, de modo que a empresa disponha do registo devidamente visado no prazo de 15 dias a contar da prestação.

4. O empregador deve manter o registo dos tempos de trabalho, bem como a declaração a que se refere o artigo 257.º e o acordo a que se refere a alínea f) do n.º 3 do artigo 226.º, durante cinco anos.

5. Constitui contraordenação grave a violação do disposto neste artigo.

(...)

CAPÍTULO VI
INCUMPRIMENTO DO CONTRATO

(...)

SECÇÃO III
PODER DISCIPLINAR

(...)

Artigo 332.º Registo das sanções disciplinares

1. O empregador deve ter um registo atualizado das sanções disciplinares, feito por forma que permita facilmente a verificação do cumprimento das disposições aplicáveis, nomeadamente por parte das autoridades competentes que solicitem a sua consulta.

2. Constitui contraordenação leve a violação do disposto no número anterior

(...)

LIVRO II
RESPONSABILIDADE PENAL E CONTRAORDENACIONAL

(...)

CAPÍTULO II
RESPONSABILIDADE CONTRAORDENACIONAL

Artigo 548.º Noção de contraordenação laboral

Constitui contraordenação laboral o facto típico, ilícito e censurável que consubstancie a violação de uma norma que consagre direitos ou imponha deveres a qualquer sujeito no âmbito de relação laboral e que seja punível com coima.

Artigo 549.º Regime das contraordenações laborais

As contraordenações laborais são reguladas pelo disposto neste Código e, subsidiariamente, pelo regime geral das contraordenações.

Artigo 550.º Punibilidade da negligência

A negligência nas contraordenações laborais é sempre punível.

Artigo 551.º Sujeito responsável por contraordenação laboral

1. O empregador é o responsável pelas contraordenações laborais, ainda que praticadas pelos seus trabalhadores no exercício das respetivas funções,

sem prejuízo da responsabilidade cometida por lei a outros sujeitos.

2.Quando um tipo contraordenacional tiver por agente o empregador abrange também a pessoa coletiva, a associação sem personalidade jurídica ou a comissão especial.

3. Se o infrator for pessoa coletiva ou equiparada, respondem pelo pagamento da coima, solidariamente com aquela, os respetivos administradores, gerentes ou diretores.

4. O contratante é responsável solidariamente pelo pagamento da coima aplicada ao subcontratante que execute todo ou parte do contrato nas instalações daquele ou sob responsabilidade do mesmo, pela violação de disposições a que corresponda uma infração muito grave, salvo se demonstrar que agiu com a diligência devida.

Artigo 552.º Apresentação de documentos
1. As pessoas singulares, coletivas e entidades equiparadas notificadas pelo serviço com competência inspetiva do ministério responsável pela área laboral para exibição, apresentação ou entrega de documentos ou outros registos ou de cópia dos mesmos devem apresentá-los no prazo e local identificados para o efeito.

2. Constitui contraordenação leve a violação do disposto no número anterior.

Artigo 553.º Escalões de gravidade das contraordenações laborais
Para determinação da coima aplicável e tendo em conta a relevância dos interesses violados, as contraordenações laborais classificam-se em leves, graves e muito graves.

Artigo 554.º Valores das coimas
1. A cada escalão de gravidade das contraordenações laborais corresponde uma coima variável em função do volume de negócios da empresa e do grau da culpa do infrator, salvo o disposto no artigo seguinte.

2. Os limites mínimo e máximo das coimas correspondentes a contraordenação leve são os seguintes:
a) Se praticada por empresa com volume de negócios inferior a (euro)

10 000 000, de 2 UC a 5 UC em caso de negligência e de 6 UC a 9 UC em caso de dolo;

b) Se praticada por empresa com volume de negócios igual ou superior a (euro) 10 000 000, de 6 UC a 9 UC em caso de negligência e de 10 UC a 15 UC em caso de dolo.

3. Os limites mínimo e máximo das coimas correspondentes a contraordenação grave são os seguintes:
a) Se praticada por empresa com volume de negócios inferior a (euro) 500 000, de 6 UC a 12 UC em caso de negligência e de 13 UC a 26 UC em caso de dolo;

b) Se praticada por empresa com volume de negócios igual ou superior a (euro) 500 000 e inferior a (euro) 2 500 000, de 7 UC a 14 UC em caso de negligência e de 15 UC a 40 UC em caso de dolo;

c) Se praticada por empresa com volume de negócios igual ou superior a (euro) 2 500 000 e inferior a (euro) 5 000 000, de 10 UC a 20 UC em caso de negligência e de 21 UC a 45 UC em caso de dolo;

d) Se praticada por empresa com volume de negócios igual ou superior a (euro) 5 000 000 e inferior a (euro) 10 000 000, de 12 UC a 25 UC em caso de negligência e de 26 UC a 50 UC em caso de dolo;

e) Se praticada por empresa com volume de negócios igual ou superior a (euro) 10 000 000, de 15 UC a 40 UC em caso de negligência e de 55 UC a 95 UC em caso de dolo.

4. Os limites mínimo e máximo das coimas correspondentes a contraordenação muito grave são os seguintes:
a) Se praticada por empresa com volume de negócios inferior a (euro) 500 000, de 20 UC a 40 UC em caso de negligência e de 45 UC a 95 UC em caso de dolo;

b) Se praticada por empresa com volume de negócios igual ou superior a (euro) 500 000 e inferior a (euro) 2 500 000, de 32 UC a 80 UC em caso de negligência e de 85 UC a 190 UC em caso de dolo;

c) Se praticada por empresa com volume de negócios igual ou superior a (euro) 2 500 000 e inferior a (euro) 5 000 000, de 42 UC a 120 UC em caso de negligência e de 120 UC a 280 UC em caso de dolo;

d) Se praticada por empresa com volume de negócios igual ou superior a (euro) 5 000 000 e inferior a (euro) 10 000 000, de 55 UC a 140 UC em caso de negligência e de 145 UC a 400 UC em caso de dolo;

e) Se praticada por empresa com volume de negócios igual ou superior a (euro) 10 000 000, de 90 UC a 300 UC em caso de negligência e de 300 UC a 600 UC em caso de dolo.

5. O volume de negócios reporta-se ao ano civil anterior ao da prática da infração.

6. Caso a empresa não tenha atividade no ano civil anterior ao da prática da infração, considera-se o volume de negócios do ano mais recente.

7. No ano de início de atividade são aplicáveis os limites previstos para empresa com volume de negócios inferior a (euro) 500 000.

8. Se o empregador não indicar o volume de negócios, aplicam-se os limites previstos para empresa com volume de negócios igual ou superior a (euro) 10 000 000.

9. A sigla UC corresponde à unidade de conta processual.

Artigo 555.º Outro valores de coimas
1. A cada escalão de gravidade das contraordenações, em caso em que o agente não tenha trabalhadores ao serviço ou, sendo pessoa singular, não exerça uma atividade com fins lucrativos corresponde o valor de coimas previsto nos números seguintes.

2. A contraordenação leve corresponde coima de 1 UC a 2 UC em caso de negligência ou de 2 UC a 3,5 UC em caso de dolo.

3. A contraordenação grave corresponde coima de 3 UC a 7 UC em caso de negligência ou de 7 UC a 14 UC em caso de dolo.

4. A contraordenação muito grave corresponde coima de 10 UC a 25 UC em caso de negligência ou de 25 UC a 50 UC em caso de dolo.

Artigo 556.º Critérios especiais de medida da coima
1. Os valores máximos das coimas aplicáveis a contraordenações muito graves previstas no n.º 4 do artigo 554.º são elevados para o dobro em situação de violação de normas sobre trabalho de menores, segurança e saúde no trabalho, direitos de estruturas de representação coletiva dos trabalhadores e direito à greve.

2. Em caso de pluralidade de agentes responsáveis pela mesma contraordenação é aplicável a coima correspondente à empresa com maior volume de negócios.

Artigo 557.º Dolo
O desrespeito de medidas recomendadas em auto de advertência é ponderado pela autoridade administrativa competente, ou pelo julgador em caso de impugnação judicial, designadamente para efeitos de aferição da existência de conduta dolosa.

Artigo 558.º Pluralidade de contraordenações
1. Quando a violação da lei afetar uma pluralidade de trabalhadores individualmente considerados, o número de contraordenações corresponde ao número de trabalhadores concretamente afetados, nos termos dos números seguintes.

2. Considera-se que a violação da lei afeta uma pluralidade de trabalhadores quando estes, no exercício da respetiva atividade, foram expostos a uma situação concreta de perigo ou sofreram dano resultante de conduta ilícita do infrator.

3. A pluralidade de infrações dá origem a um processo e as infrações são sancionadas com uma coima única que não pode exceder o dobro da coima máxima aplicável em concreto.

4. Se, com a infração praticada, o agente obteve um benefício económico, este deve ser tido em conta na determinação da medida da coima nos termos do disposto no artigo 18.º do regime geral das contraordenações, na redação dada pelo Decreto-Lei n.º 244/95, de 14 de Setembro.

Artigo 559.º Determinação da medida da coima
1. Na determinação da medida da coima, além do disposto no regime geral das contraordenações, são ainda atendíveis a medida do incumprimento das recomendações constantes de auto de advertência, a coação, falsificação, simulação ou outro meio fraudulento usado pelo agente.

2. No caso de violação de normas de segurança e saúde no trabalho, são também atendíveis os princípios gerais de prevenção a que devem obedecer as medidas de proteção, bem como a permanência ou transitoriedade da infração, o número de trabalhadores potencialmente afetados e as medidas e instruções adotadas pelo empregador para prevenir os riscos.

3. Cessando o contrato de trabalho, no caso de o arguido cumprir o disposto no artigo 245.º e proceder ao pagamento voluntário da coima por violação do disposto no n.º 1 ou 5 do artigo 238.º, no n.º 1, 4 ou 5 do artigo 239.º ou no n.º 1, 2 ou 3 do artigo 244.º, esta é liquidada pelo valor correspondente à contraordenação leve.

Artigo 560.º Dispensa da coima
A coima prevista para as contraordenações referidas no n.º 4 do artigo 353.º, no n.º 2 do artigo 355.º, no n.º 7 do artigo 356.º, no n.º 8 do artigo 357.º, no n.º 6 do artigo 358.º, no n.º 6 do artigo 360.º, no n.º 6 do artigo 361.º, no n.º 6 do artigo 363.º, no n.º 6 do artigo 368.º, no n.º 2 do artigo 369.º, no n.º 5 do artigo 371.º, no n.º 8 do artigo 375.º, no n.º 3 do artigo 376.º, no n.º 3 do artigo 378.º e no n.º 3 do artigo 380.º, na parte em que se refere a violação do n.º 1 do mesmo artigo, não se aplica caso o empregador assegure ao trabalhador os direitos a que se refere o artigo 389.º

Artigo 561.º Reincidência
1. É sancionado como reincidente quem comete uma contraordenação grave praticada com dolo ou uma contraordenação muito grave, depois de ter sido condenado por outra contraordenação grave praticada com dolo ou contraordenação muito grave, se entre as duas infrações tiver decorrido um prazo não superior ao da prescrição da primeira.

2. Em caso de reincidência, os limites mínimo e máximo da coima são elevados em um terço do respetivo valor, não podendo esta ser inferior ao valor da coima aplicada pela contraordenação anterior desde que os limites mínimo e máximo desta não sejam superiores aos daquela.

Artigo 562.º Sanções acessórias
1. No caso de contraordenação muito grave ou reincidência em contraordenação grave, praticada com dolo ou negligência grosseira, é aplicada ao agente a sanção acessória de publicidade.

2. No caso de reincidência em contraordenação prevista no número anterior, tendo em conta os efeitos gravosos para o trabalhador ou o benefício económico retirado pelo empregador com o incumprimento, podem ainda ser aplicadas as seguintes sanções acessórias:
a) Interdição do exercício de atividade no estabelecimento, unidade fabril ou estaleiro onde se verificar a infração, por um período até dois anos;

b) Privação do direito de participar em arrematações ou concursos públicos, por um período até dois anos.

3. A publicidade da decisão condenatória consiste na inclusão em registo público, disponibilizado na página eletrónica do serviço com competência inspetiva do ministério responsável pela área laboral, de um extrato com a caracterização da contraordenação, a norma violada, a identificação do infrator, o sector de atividade, o lugar da prática da infração e a sanção aplicada.

4. A publicidade referida no número anterior é promovida pelo tribunal competente, em relação a contraordenação objeto de decisão judicial, ou pelo serviço referido no mesmo número, nos restantes casos.

Artigo 563.º Dispensa e eliminação da publicidade
1. A sanção acessória de publicidade pode ser dispensada, tendo em conta as circunstâncias da infração, se o agente tiver pago imediatamente a coima a que foi condenado e se não tiver praticado qualquer contraordenação grave ou muito grave nos cinco anos anteriores.

2. Decorrido um ano desde a publicidade da decisão condenatória sem que o agente tenha sido novamente condenado por contraordenação grave ou muito grave, é a mesma eliminada do registo referido no artigo anterior.

Artigo 564.º Cumprimento de dever omitido
1. Sempre que a contraordenação laboral consista na omissão de um dever, o pagamento da coima não dispensa o infrator do seu cumprimento se este ainda for possível.

2. A decisão que aplique a coima deve conter, sendo caso disso, a ordem de pagamento de quantitativos em dívida ao trabalhador, a efetuar dentro do prazo estabelecido para o pagamento da coima.

3. Em caso de não pagamento, a decisão referida no número anterior serve de base à execução efetuada nos termos do artigo 89.º do regime geral das contraordenações, na redação dada pelo Decreto-Lei n.º 244/95, de 14 de Setembro, aplicando-se as normas do processo comum de execução para pagamento de quantia certa.

Artigo 565.º Registo individual
1. O serviço com competência inspetiva do ministério responsável pela área laboral organiza um registo individual dos sujeitos responsáveis pelas contraordenações laborais, de âmbito nacional, do qual constam as infrações praticadas, as datas em que foram cometidas, as coimas e as sanções acessórias aplicadas, assim como as datas em que as decisões condenatórias se tornaram irrecorríveis.

2. Os tribunais e os departamentos das administrações regionais dos Açores e da Madeira com competência para a aplicação de coimas remetem ao serviço referido no número anterior os elementos neste indicados.

Artigo 566.º Destino das coimas
1. Em processo cuja instrução esteja cometida ao serviço com competência inspectiva do ministério responsável pela área laboral, metade do produto da coima aplicada reverte para este, a título de compensação de custos de funcionamento e despesas processuais, tendo o remanescente o seguinte destino:
a) Fundo de Acidentes de Trabalho, no caso de coima aplicada em matéria de segurança e saúde no trabalho;

b) 35 % para o serviço responsável pela gestão financeira do orçamento da segurança social e 15 % para o Orçamento do Estado, relativamente a outra coima.

2. O serviço referido no número anterior transfere trimestralmente para as entidades referidas no número anterior as importâncias a que têm direito.

8. Lei n.º 43/2004, 18 de Agosto - Lei de Organização e funcionamento da Comissão Nacional de Proteção de Dados[7]

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º Âmbito
A presente lei regula a organização e o funcionamento da Comissão Nacional de Proteção de Dados (CNPD), bem como o estatuto pessoal dos seus membros.

Artigo 2.º Natureza, atribuições e competências
A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República, com as atribuições e competências definidas na lei.

CAPÍTULO II
MEMBROS DA CNPD

Artigo 3.º Designação e mandato
1. Os membros da CNPD são designados nos termos previstos no artigo 25.º da Lei n.º 67/98, de 26 de Outubro.

2. O mandato dos membros da CNPD é de cinco anos e cessa com a posse dos novos membros, não podendo ser renovado por mais de uma vez.

Artigo 4.º Incapacidades e incompatibilidades
1. Só podem ser membros da CNPD os cidadãos que se encontrem no pleno gozo dos seus direitos civis e políticos.

2. Os membros da CNPD ficam sujeitos ao regime de incompatibilidades estabelecido para os titulares de altos cargos públicos.

Artigo 5.º Inamovibilidade
1. Os membros da CNPD são inamovíveis, não podendo as suas funções cessar antes do termo do mandato, salvo nos seguintes casos:
a) Morte ou impossibilidade física permanente ou com uma duração que se preveja ultrapassar a data do termo do mandato;

[7] *Última modificação legislativa: Lei n.º 55-A/2010, de 31 de Dezembro*

b) Renúncia ao mandato;

c) Perda do mandato.

2. No caso de vacatura por um dos motivos previstos no número anterior, a vaga deve ser preenchida no prazo de 30 dias após a sua verificação, através da designação de novo membro pela entidade competente.

3. O membro designado nos termos do número anterior completa o mandato do membro que substitui.

Artigo 6.º Renúncia
1. Os membros da CNPD podem renunciar ao mandato através de declaração escrita apresentada à Comissão.

2. A renúncia torna-se efetiva com o seu anúncio e é publicada na 2.ª série do Diário da República.

Artigo 7.º Perda do mandato
1. Perdem o mandato os membros da CNPD que:
a) Sejam abrangidos por qualquer das incapacidades ou incompatibilidades previstas na lei;

b) Faltem, no mesmo ano civil, a três reuniões consecutivas ou a seis interpoladas, salvo motivo justificado;

c) Cometam violação do disposto na alínea c) do artigo 8.º, desde que judicialmente declarada.

2. A perda do mandato é objeto, conforme os casos, de deliberação ou declaração a publicar na 2.ª série do Diário da República.

Artigo 8.º Deveres
Constituem deveres dos membros da CNPD:
a) Exercer o respetivo cargo com isenção, rigor e independência;

b) Participar ativa e assiduamente nos trabalhos do órgão que integram;

c) Guardar sigilo sobre as questões ou processos que estejam a ser objeto

de apreciação, sem prejuízo das obrigações a que se referem os artigos 11.º e 17.º da Lei n.º 67/98, de 26 de Outubro.

Artigo 9.º Estatuto remuneratório
1. O presidente da CNPD é remunerado de acordo com a tabela indiciária e o regime fixados para o cargo de diretor-geral, cabendo aos restantes membros uma remuneração igual a 85% daquela, sem prejuízo da faculdade de opção pelas remunerações correspondentes ao lugar de origem.

2. O presidente da CNPD tem direito a um abono mensal para despesas de representação de montante igual ao atribuído aos diretores-gerais.

3. Os restantes membros da CNPD têm direito a um abono mensal para despesas de representação de montante igual ao atribuído aos subdiretores-gerais.

4. Os membros da CNPD beneficiam do regime geral de segurança social, se não estiverem abrangidos por outro mais favorável.

Artigo 10.º Garantias
Os membros da CNPD beneficiam das seguintes garantias:
a) Não podem ser prejudicados na estabilidade do seu emprego, na sua carreira profissional e no regime de segurança social de que beneficiem;

b) O período correspondente ao exercício do mandato considera-se, para todos os efeitos legais, como prestado no lugar de origem;

c) O período de duração do mandato suspende, a requerimento do interessado, a contagem dos prazos para a apresentação de relatórios curriculares ou prestação de provas para a carreira de docente de ensino superior ou para a de investigação científica, bem como a contagem dos prazos dos contratos de professores convidados, assistentes, assistentes estagiários ou convidados;

d) Têm direito a ser dispensados das suas atividades públicas ou privadas, quando se encontrem em funções de representação nacional ou internacional da Comissão.

Artigo 11.º Impedimentos e suspeições
1. Aos impedimentos e suspeições são aplicáveis, com as devidas adaptações, as disposições do Código do Procedimento Administrativo.

2. Os impedimentos e suspeições são apreciados pela CNPD.

Artigo 12.º Cartão de identificação
1. Os membros da CNPD possuem cartão de identificação, dele constando o cargo as regalias e os direitos inerentes à sua função.

2. O cartão de identificação é simultaneamente de livre-trânsito e de acesso a todos os locais em que sejam tratados dados pessoais sujeitos ao controlo da CNPD.

CAPÍTULO III
FUNCIONAMENTO DA CNPD

Artigo 13.º Reuniões
1. A CNPD funciona com carácter permanente.

2. A CNPD tem reuniões ordinárias e extraordinárias.

3. As reuniões extraordinárias têm lugar:
a) Por iniciativa do presidente;

b) A pedido de três dos seus membros.

4. As reuniões da CNPD não são públicas e realizam-se nas suas instalações ou, por sua deliberação, em qualquer outro local do território nacional, sendo a periodicidade estabelecida nos termos adequados ao desempenho das suas funções.

5. O presidente, quando o entender conveniente, pode, com o acordo da Comissão, convidar a participar nas reuniões, salvo na fase decisória, qualquer pessoa cuja presença seja considerada útil.

6. Das reuniões é lavrada ata, que, depois de aprovada pela CNPD, é assinada pelo presidente e pelo secretário.

Artigo 14.º Ordem de trabalhos
1. A ordem de trabalhos para cada reunião ordinária é fixada pelo presidente, devendo ser comunicada aos vogais com a antecedência mínima de dois dias úteis relativamente à data prevista para a sua realização.

2. A ordem de trabalhos deve incluir os assuntos que para esse fim lhe forem indicados por qualquer vogal, desde que sejam da competência do órgão e o pedido seja apresentado por escrito com uma antecedência mínima de cinco dias sobre a data da reunião.

Artigo 15.º Deliberações
1. A CNPD só pode reunir e deliberar com a presença de pelo menos quatro membros.

2. As deliberações da CNPD são tomadas por maioria dos membros presentes, tendo o presidente voto de qualidade.

3. Carecem, porém, de aprovação por maioria dos membros em efetividade de funções as deliberações a que se refere o n.º 3 do artigo 19.º, o n.º 2 do artigo 20.º, o n.º 4 do artigo 22.º, a parte final das alíneas f) e l) do n.º 1 do artigo 23.º, o n.º 2 do artigo 27.º, a alínea a) do n.º 1 do artigo 28.º e o n.º 3 do artigo 32.º, todos da Lei n.º 67/98, de 26 de Outubro, e ainda o n.º 2 do artigo 21.º da presente lei.

Artigo 16.º Publicidade das deliberações
São publicadas na 2.ª série do Diário da República:
a) As autorizações referidas na alínea h) do n.º 1 do artigo 23.º da Lei n.º 67/98, de 26 de Outubro;

b) As autorizações previstas no n.º 2 do artigo 27.º da Lei n.º 67/98, de 26 de Outubro;

c) As deliberações que aprovem as diretivas a que se referem as alíneas f) e l) do n.º 1 do artigo 23.º da Lei n.º 67/98, de 26 de Outubro;

d) As deliberações que fixem taxas nos termos do n.º 2 do artigo 21.º da presente lei.

Artigo 17.º Reclamações, queixas e petições
1. As reclamações, queixas e petições são dirigidas por escrito à CNPD, com indicação do nome e endereço dos seus autores, podendo ser exigida a confirmação da identidade destes.

2. O direito de petição pode ser exercido por correio tradicional ou eletrónico, ou através de telégrafo, telefax e outros meios de comunicação.

3. Quando a questão suscitada não for da competência da CNPD, deve a mesma ser encaminhada para a entidade competente, com informação ao exponente.

4. As reclamações, queixas e petições manifestamente infundadas podem ser arquivadas pelo membro da Comissão a quem o respetivo processo tenha sido distribuído.

Artigo 18.º Formalidades
1. Os documentos dirigidos à CNPD e o processado subsequente não estão sujeitos a formalidades especiais.

2. A CNPD pode aprovar modelos ou formulários, em suporte papel ou electrónico, com vista a permitir melhor instrução dos pedidos de parecer ou de autorização, bem como das notificações de tratamentos de dados pessoais.

3. Os pedidos de autorização e as notificações apresentados à CNPD nos termos do artigo 29.º da Lei n.º 67/98, de 26 de Outubro, devem ser assinados pelo responsável do tratamento de dados pessoais ou pelo seu legal representante.

4 - Os pedidos de parecer sobre iniciativas legislativas devem ser remetidos à CNPD pelo titular do órgão legiferante.

5. Os pedidos de parecer sobre quaisquer outros instrumentos jurídicos comunitários ou internacionais em preparação, relativos ao tratamento de dados pessoais, devem ser remetidos à CNPD pela entidade que representa o Estado Português no processo de elaboração da iniciativa.

Artigo 19.º Competências e substituição do presidente
1. Compete ao presidente:
a) Representar a Comissão;

b) Superintender nos serviços de apoio;

c) Convocar as sessões e fixar a ordem de trabalhos;

d) Ouvida a Comissão, nomear o pessoal do quadro e autorizar transferências, requisições e destacamentos;

e) Ouvida a Comissão, autorizar a contratação do pessoal referido no n.º 5 do artigo 30.º;

f) Outorgar contratos em nome da Comissão e obrigá-la nos demais negócios jurídicos;

g) Autorizar a realização de despesas dentro dos limites legalmente compreendidos na competência dos ministros;

h) Aplicar coimas e homologar deliberações, nos termos previstos na lei;

i) Ouvida a Comissão, fixar as regras de distribuição dos processos;

j) Submeter à aprovação da Comissão o plano de atividades;

l) Em geral, assegurar o cumprimento das leis e a regularidade das deliberações.

2. O presidente é substituído, nas suas faltas e impedimentos, pelo vogal que a Comissão designar.

CAPÍTULO IV
REGIME FINANCEIRO

Artigo 20.º Regime de receitas e despesas
1. As receitas e despesas da CNPD, que goza de autonomia administrativa, constam de orçamento anual.

2. Além das dotações que lhe sejam atribuídas no Orçamento da Assembleia da República, nos termos da Lei n.º 59/90, de 21 de Novembro, constituem receitas da Comissão Nacional de Proteção de Dados a inscrever diretamente no Orçamento do Estado:
a) O produto das taxas cobradas;

b) O produto da venda de formulários e publicações;

c) O produto dos encargos da passagem de certidões e acesso a documentos;

d) A parte que lhe cabe no produto das coimas, nos termos previstos na lei;

e) O saldo de gerência do ano anterior;

f) Os subsídios, subvenções, comparticipações, doações e legados, concedidos por entidades, públicas e privadas, nacionais, estrangeiras, comunitárias ou internacionais;

g) Quaisquer outras receitas que lhe sejam atribuídas por lei ou contrato.

3. Constituem despesas da CNPD as que resultem dos encargos e responsabilidades decorrentes do seu funcionamento, bem como quaisquer outras relativas à prossecução das suas atribuições.

4. O orçamento anual, as respetivas alterações bem como as contas são aprovados pela CNPD.

5. As contas da CNPD ficam sujeitas, nos termos gerais, ao controlo do Tribunal de Contas.

Artigo 21.º Taxas
1. A CNPD pode cobrar taxas:
a) Pelo registo das notificações;

b) Pelas autorizações concedidas ao abrigo do disposto no artigo 28.º da Lei n.º 67/98, de 26 de Outubro, ou outras autorizações legalmente previstas.

2. O montante das taxas, que deve ser proporcional à complexidade do pedido e ao serviço prestado é fixado pela CNPD e não pode ser superior a

metade do salário mínimo nacional dos trabalhadores por conta de outrem.

3. Em caso de comprovada insuficiência económica, o interessado poderá ficar isento, total ou parcialmente, do pagamento das taxas referidas no n.º 1, mediante deliberação da CNPD.

CAPÍTULO V
SERVIÇOS DE APOIO

Artigo 22.º Organização dos serviços de apoio
1. A CNPD dispõe de serviços de apoio próprios.

2. Os serviços de apoio compreendem:
a) Serviço Jurídico (SJ);

b) Serviço de Informação e Relações Internacionais (SIRI);

c) Serviço de Informática e Inspeção (SII);

d) Serviço de Apoio Administrativo e Financeiro (SAAF).

3. Os serviços de apoio são dirigidos por um secretário, o qual tem direito à remuneração mais elevada de consultor-coordenador, bem como a um abono mensal para despesas de representação no valor de 8% da remuneração base.

4. O secretário é nomeado por despacho do presidente, obtido parecer favorável da Comissão, com observância dos requisitos legais adequados ao desempenho das respetivas funções, escolhido preferencialmente de entre funcionários já pertencentes ao quadro da CNPD, habilitados com licenciatura e de reconhecida competência para o desempenho do lugar.

5. A nomeação do secretário é feita em regime de comissão de serviço, por períodos de três anos.

Artigo 23.º Competências do secretário
1. Compete ao secretário:
a) Secretariar a Comissão;

b) Dar execução às decisões da Comissão, de acordo com as orientações do presidente;

c) Assegurar a boa organização e funcionamento dos serviços de apoio, nomeadamente no tocante à gestão financeira, do pessoal e das instalações e equipamento, de acordo com as orientações do presidente;

d) Elaborar o projeto de orçamento, bem como as respetivas alterações, e assegurar a sua execução;

e) Elaborar o projeto de relatório anual.

2. O secretário é substituído, nas suas faltas e impedimentos, pelo técnico superior ou consultor designado pelo presidente, obtido parecer favorável da Comissão.

Artigo 24.º Serviço Jurídico
Compete ao SJ assegurar o apoio técnico-jurídico, designadamente:
a) Preparar pareceres sobre projetos legislativos;

b) Instruir os processos de registo ou autorização de tratamento de dados pessoais e assegurar a respetiva tramitação;

c) Instruir os processos de contraordenação, bem como os relativos a queixas, reclamações e petições;

d) Colaborar na organização de colóquios, seminários e outras iniciativas de difusão das matérias de proteção da vida privada e dos dados pessoais;

e) Coadjuvar os membros da CNPD na participação em atividades de organizações comunitárias ou internacionais;

f) Desempenhar quaisquer outras tarefas de âmbito técnico-jurídico.

Artigo 25.º Serviço de Informação e Relações Internacionais
Compete ao SIRI assegurar o apoio em matérias de informação, documentação e relações públicas, designadamente:
a) Promover a difusão dos princípios da proteção da vida privada e dos dados pessoais e dos diplomas legislativos e instrumentos comunitários

e internacionais correspondentes;

b) Assegurar os contactos com os órgãos de comunicação social;

c) Organizar e dinamizar a realização de colóquios, seminários e outras iniciativas;

d) Organizar e manter atualizado o centro de documentação;

e) Colaborar na conceção e edição de publicações, bem como no relatório anual de atividades;

f) Colaborar no apoio aos membros da CNPD na participação em atividades de organizações nacionais, comunitárias ou internacionais;

g) Desempenhar quaisquer outras tarefas, no âmbito da informação, da documentação e das relações internacionais.

Artigo 26.º Serviço de Informática e Inspeção
Compete ao SII garantir o normal funcionamento do sistema de informação da CNPD e disponibilizar o apoio técnico considerado necessário na área das tecnologias de informação, nomeadamente:
a) Assegurar a gestão do sistema de informação, proporcionando o necessário ambiente operativo (suporte lógico e suporte físico) de acordo com as orientações da CNPD;

b) Garantir os meios técnicos necessários para a criação e manutenção do registo público previsto no artigo 31.º da Lei n.º 67/98, de 26 de Outubro;

c) Propor e zelar pela aplicação de normas de segurança que garantam a fiabilidade, confidencialidade e durabilidade do sistema de informação;

d) Apoiar a gestão do sítio da CNPD, garantindo, em particular, a sua manutenção técnica;

e) Realizar ações de inspeção e de auditoria informática a sistemas de informação, no âmbito de processos em curso, com mandato de qualquer dos membros da CNPD;

f) Colaborar no apoio aos membros da CNPD na participação em atividades de organizações nacionais, comunitárias ou internacionais;

g) Desempenhar quaisquer outras tarefas, no âmbito da utilização das tecnologias de informação e comunicação.

Artigo 27.º Serviço de Apoio Administrativo e Financeiro
Compete ao SAAF apoiar a CNPD na gestão dos processos e dos recursos humanos, financeiros e materiais, designadamente:
a) Organizar e assegurar toda a tramitação dos processos;

b) Promover o recrutamento, promoção e formação do pessoal, bem como a aplicação dos instrumentos de mobilidade e a contratação de pessoal;

c) Preparar as propostas de orçamento e acompanhar a sua execução;

d) Assegurar o processamento e a contabilização das receitas e das despesas;

e) Elaborar a conta de gerência e o respetivo relatório;

f) Promover as aquisições de bens e serviços, administrar os bens de consumo, bem como gerir as instalações, viaturas e demais equipamentos ao serviço da CNPD;

g) Desempenhar quaisquer outras tarefas de que, no âmbito das suas áreas de intervenção, seja encarregado pelo presidente ou pelo secretário.

Artigo 28.º Regime de pessoal
1. Ao pessoal da CNPD aplica-se o regime geral da função pública.

2. O pessoal da CNPD está isento de horário de trabalho, não sendo por isso devida qualquer remuneração a título de horas extraordinárias, sem prejuízo do disposto no artigo 33.º

Artigo 29.º Cartão de identificação
Os funcionários da CNPD possuem cartão de identificação, dele constando o cargo desempenhado e os direitos e regalias inerentes à sua função.

CAPÍTULO VI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Artigo 30.º Quadro de pessoal
1. O quadro de pessoal, bem como o conteúdo funcional das respetivas carreiras, é fixado em resolução da Assembleia da República.

2. Os lugares de consultor da CNPD serão providos em regime de comissão de serviço, por tempo indeterminado, requisição ou destacamento, no caso da nomeação recair em funcionário público, ou em regime de contrato individual de trabalho, quando não vinculados à Administração Pública.

3. São condições indispensáveis ao recrutamento de consultor a elevada competência profissional e experiência válida para o exercício da função, a avaliar com base nos respetivos curricula.

4. O prazo previsto no n.º 3 do artigo 27.º do Decreto-Lei n.º 427/89, de 7 de Dezembro, não é aplicável ao regime de requisição ou destacamento aos serviços de apoio à CNPD, podendo porém a comissão de serviço, destacamento ou requisição ser dada por finda por decisão do presidente, ouvida a Comissão, ou a pedido do interessado.

5. Quando a complexidade e ou especificidade dos assuntos o exigir pode o presidente autorizar a contratação de pessoal em regime de contrato de prestação de serviços.

Artigo 31.º Funcionários e agentes
A nomeação em comissão de serviço de funcionários da Administração Pública para o cargo de consultor não determina a abertura de vaga no quadro de origem, ficando salvaguardados todos os direitos inerentes aos seus anteriores cargos ou funções, designadamente para efeitos de promoção ou progressão.

Artigo 32.º Remuneração base, recrutamento, promoção e progressão dos consultores
1. A remuneração base mensal dos consultores da CNPD consta do mapa I anexo a esta lei, de que faz parte integrante.

2. A promoção e progressão nas categorias de consultor-coordenador e consultor rege-se pelos princípios aplicáveis à carreira técnica superior.

3. Pode haver lugar a recrutamento direto para a categoria de consultor-coordenador, desde que os candidatos possuam adequada qualificação e experiência profissional para o efeito.

4. Podem ser recrutados como consultores-adjuntos indivíduos licenciados com qualificações para o exercício da função, sempre que não se justifique o recrutamento na categoria de consultor.

Artigo 33.º Disponibilidade permanente
1. O pessoal da CNPD tem direito a um suplemento remuneratório, a título de disponibilidade permanente, de montante mensal correspondente a 12,5% da remuneração base.

2. O suplemento é abonado em 12 mensalidades e releva para efeitos de aposentação, sendo considerado no cálculo da pensão pela fórmula prevista na alínea b) do n.º 1 do artigo 47.º do Estatuto da Aposentação.

3. Ao pessoal da CNPD abrangido pelos n.os 1, 2, 7 e 9 do artigo 34.º não é atribuído o suplemento referido nos números anteriores.

Artigo 34.º Pessoal atualmente ao serviço da CNPD
1. Os funcionários e agentes que prestam atualmente serviço na CNPD e que beneficiam do regime do n.º 3 do artigo 26.º da Lei n.º 67/98, de 26 de Outubro, transitam para o novo quadro de acordo com as regras dos números seguintes, mantendo o seu atual estatuto remuneratório, que passa a ter a natureza de remuneração pessoal.

2. Ao pessoal da CNPD, não vinculado à Administração Pública, que se encontre na situação do número anterior aplica-se idêntico regime remuneratório, sendo porém a sua relação jurídica de emprego a do contrato individual de trabalho, ao abrigo da lei geral aplicável à Administração Pública.

3. Os lugares da carreira técnica superior e especialista de informática previstos no quadro de pessoal, para garantir a transição prevista nos n.os 1 e 2, são lugares a extinguir quando vagarem.

4. Os funcionários vinculados à Administração Pública a prestar serviço na CNPD à data da entrada em vigor da presente lei transitam para o novo quadro, mediante deliberação daquela, para a carreira e categoria que integre as funções que o funcionário efetivamente desempenhe, sem prejuízo das habilitações e qualificações legalmente exigidas, em escalão a que corresponda o mesmo índice remuneratório, ou, quando não houver coincidência de índice, em escalão a que corresponda o índice superior mais aproximado na estrutura da carreira para que se processe a transição.

5. A correspondência referida no número anterior fixa-se entre os índices remuneratórios definidos para o escalão 1 da categoria em que o funcionário se encontra e o escalão 1 da categoria da nova carreira.

6. Aos funcionários que, nos termos do n.º 1, transitem para categoria diversa será contado, nesta última, para todos os efeitos legais, o tempo de serviço prestado na anterior, desde que no exercício de funções idênticas ou semelhantes às da nova carreira.

7. O disposto no n.º 1 aplica-se igualmente ao atual secretário, com as necessárias adaptações decorrentes do regime de exercício de funções.

8. A transição para os lugares do quadro da CNPD faz-se por despacho do presidente, independentemente de quaisquer outras formalidades, sem prejuízo do disposto no n.º 1.

9. A CNPD pode deliberar manter as comissões, requisições ou destacamentos do pessoal ao seu serviço à data da entrada em vigor da presente lei, mantendo os funcionários que beneficiem do n.º 3 do artigo 26.º da Lei n.º 67/98 o seu atual estatuto remuneratório, que passa a ter natureza de remuneração pessoal.

Artigo 35.º Norma transitória

1. A suspensão da comissão de serviço do presidente da CNPD mantém-se até ao termo do seu mandato.

2. A aplicação da presente lei no corrente ano faz-se no quadro orçamental aprovado para a CNPD em 2004.

Artigo 36.º Norma revogatória
São revogados:
a) O Decreto-Lei n.º 121/93, de 16 de Abril;

b) A Resolução da Assembleia da República n.º 53/94, de 19 de Agosto.

Aprovada em 8 de Julho de 2004.
O Presidente da Assembleia da República,
João Bosco Mota Amaral.
Promulgada em 2 de Agosto de 2004.
Publique-se.
O Presidente da República,
JORGE SAMPAIO.
Referendada em 5 de Agosto de 2004.
O Primeiro-Ministro,
Pedro Miguel de Santana Lopes.

ANEXO
MAPA I
(a que se refere o n.º 1 do artigo 32.º)

	1	**2**	**3**
Consultor-Coordenador	770	830	900
Consultor	690	730	770
Consultor-Adjunto	500		

9. Decreto-lei nº 7/2004 de 7 de Janeiro, transpõe para a ordem jurídca nacional a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno[8] - Lei do Comércio Eletrónico

1.

O presente diploma destina-se fundamentalmente a realizar a transposição da Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000.

A diretiva sobre comércio eletrónico, não obstante a designação, não regula todo o comércio eletrónico: deixa amplas zonas em aberto ou porque fazem parte do conteúdo de outras diretivas ou porque não foram consideradas suficientemente consolidadas para uma harmonização comunitária ou, ainda, porque não carecem desta. Por outro lado, versa sobre matérias como a contratação eletrónica, que só tem sentido regular como matéria de direito comum e não apenas comercial.

Na tarefa de transposição, optou-se por afastar soluções mais amplas e ambiciosas para a regulação do sector em causa, tendo-se adotado um diploma cujo âmbito é fundamentalmente o da diretiva. Mesmo assim, aproveitou-se a oportunidade para, lateralmente, versar alguns pontos carecidos de regulação na ordem jurídica portuguesa que não estão contemplados na diretiva.

A transposição apresenta a dificuldade de conciliar categorias neutras próprias de uma directiva, que é um concentrado de sistemas jurídicos diferenciados, com os quadros vigentes na nossa ordem jurídica. Levou-se tão longe quanto possível a conciliação da fidelidade à diretiva com a integração nas categorias portuguesas para tornar a disciplina introduzida compreensível para os seus destinatários. Assim, a própria sistemática da diretiva é alterada e os conceitos são vertidos, sempre que possível, nos quadros correspondentes do direito português.

---

[8] Última modificação legislativa: Lei n.º 46/2012, de 29 de Agosto, transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

2.

A diretiva pressupõe o que é já conteúdo de diretivas anteriores. Particularmente importante é a diretiva sobre contratos à distância, já transposta para a lei portuguesa pelo Decreto-Lei n.º 143/2001, de 26 de Abril. Parece elucidativo declarar expressamente o carácter subsidiário do diploma de transposição respetivo. O mesmo haverá que dizer da diretiva sobre a comercialização à distância de serviços financeiros, que está em trabalhos de transposição.

Uma das finalidades principais da diretiva é assegurar a liberdade de estabelecimento e de exercício da prestação de serviços da sociedade da informação na União Europeia, embora com as limitações que se assinalam. O esquema adotado consiste na subordinação dos prestadores de serviços à ordenação do Estado membro em que se encontram estabelecidos. Assim se fez, procurando esclarecer quanto possível conceitos expressos em linguagem generalizada mas pouco precisa como «serviço da sociedade da informação». Este é entendido como um serviço prestado a distância por via eletrónica, no âmbito de uma atividade económica, na sequência de pedido individual do destinatário o que exclui a radiodifusão sonora ou televisiva.

O considerando 57) da Diretiva n.º 2000/31/CE recorda que «o Tribunal de Justiça tem sustentado de modo constante que um Estado membro mantém o direito de tomar medidas contra um prestador de serviços estabelecido noutro Estado membro, mas que dirige toda ou a maior parte das suas atividades para o território do primeiro Estado membro, se a escolha do estabelecimento foi feita no intuito de iludir a legislação que se aplicaria ao prestador caso este se tivesse estabelecido no território desse primeiro Estado membro».

3.

Outro grande objetivo da diretiva consiste em determinar o regime de responsabilidade dos prestadores intermediários de serviços. Mais precisamente, visa-se estabelecer as condições de irresponsabilidade destes prestadores face à eventual ilicitude das mensagens que disponibilizam.

Há que partir da declaração da ausência de um dever geral de vigilância do prestador intermediário de serviços sobre as informações que transmite ou armazena ou a que faculte o acesso. Procede-se também ao enunciado dos deveres comuns a todos os prestadores intermediários de serviços.

Segue-se o traçado do regime de responsabilidade específico das atividades que a própria diretiva enuncia: simples transporte, armazenagem intermediária e armazenagem principal. Aproveitou-se a oportunidade para prever já a situação dos prestadores intermediários de serviços de associação de conteúdos (como os instrumentos de busca e as hiperconexões), que é assimilada à dos prestadores de serviços de armazenagem principal.
Introduz-se um esquema de resolução provisória de litígios que surjam quanto à licitude de conteúdos disponíveis em rede, dada a extrema urgência que pode haver numa composição prima facie. Confia-se essa função à entidade de supervisão respetiva, sem prejuízo da solução definitiva do litígio, que só poderá ser judicial.

4.

A diretiva regula também o que se designa como comunicações comerciais. Parece preferível falar de «comunicações publicitárias em rede», uma vez que é sempre e só a publicidade que está em causa.
Aqui surge a problemática das comunicações não solicitadas, que a diretiva deixa em grande medida em aberto. Teve-se em conta a circunstância de entretanto ter sido aprovada a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (diretiva relativa à privacidade e às comunicações eletrónicas), que aguarda transposição. O artigo 13.º desta respeita a comunicações não solicitadas, estabelecendo que as comunicações para fins de marketing direto apenas podem ser autorizadas em relação a destinatários que tenham dado o seu consentimento prévio. O sistema que se consagra inspira-se no aí estabelecido. Nessa medida este diploma também representa a transposição parcial dessa diretiva no que respeita ao artigo 13.º (comunicações não solicitadas).

5.

A contratação eletrónica representa o tema de maior delicadeza desta diretiva. Esclarece-se expressamente que o preceituado abrange todo o tipo de contratos, sejam ou não qualificáveis como comerciais.
O princípio instaurado é o da liberdade de recurso à via eletrónica, para que a lei não levante obstáculos, com as exceções que se apontam. Para isso haverá que afastar o que se oponha a essa celebração.

Particularmente importante se apresentava a exigência de forma escrita. Retoma-se a fórmula já acolhida no artigo 4.º do Código dos Valores Mobiliários que é ampla e independente de considerações técnicas: as declarações emitidas por via eletrónica satisfazem as exigências legais de forma escrita quando oferecem as mesmas garantias de fidedignidade, inteligibilidade e conservação.

Outro ponto muito sensível é o do momento da conclusão do contrato. A diretiva não o versa, porque não se propõe harmonizar o direito civil. Os Estados membros têm tomado as posições mais diversas. Particularmente, está em causa o significado do aviso de receção da encomenda, que pode tomar-se como aceitação ou não.

Adota-se esta última posição, que é maioritária, pois o aviso de receção destina-se a assegurar a efetividade da comunicação eletrónica, apenas, e não a exprimir uma posição negocial. Mas esclarece-se também que a oferta de produtos ou serviços em linha representa proposta contratual ou convite a contratar, consoante contiver ou não todos os elementos necessários para que o contrato fique concluído com a aceitação.

Procura também regular-se a chamada contratação entre computadores, portanto a contratação inteiramente automatizada, sem intervenção humana. Estabelece-se que se regula pelas regras comuns enquanto estas não pressupuserem justamente a atuação (humana). Esclarece-se também em que moldes são aplicáveis nesse caso as disposições sobre erro.

6.

Perante a previsão na diretiva do funcionamento de mecanismos de resolução extrajudicial de litígios, inclusive através dos meios eletrónicos adequados, houve que encontrar uma forma apropriada de transposição deste princípio.

As muitas funções atribuídas a entidades públicas aconselham a previsão de entidades de supervisão. Quando a competência não couber a entidades especiais, funciona uma entidade de supervisão central: essa função é desempenhada pela ICP-ANACOM. As entidades de supervisão têm funções no domínio da instrução dos processos contraordenacionais, que se preveem, e da aplicação das coimas respetivas.

O montante das coimas é fixado entre molduras muito amplas, de modo a serem dissuasoras, mas, simultaneamente, se adequarem à grande variedade de situações que se podem configurar.

Às contraordenações podem estar associadas sanções acessórias; mas as sanções acessórias mais graves terão necessariamente de ser confirmadas em juízo, por iniciativa oficiosa da própria entidade de supervisão.
Prevêem-se providências provisórias, a aplicar pela entidade de supervisão competente, e que esta pode instaurar, modificar e levantar a todo o momento.
Enfim, é ainda objetivo deste diploma permitir o recurso a meios de solução extrajudicial de litígios para os conflitos surgidos neste domínio, sem que a legislação geral traga impedimentos, nomeadamente à solução destes litígios por via eletrónica.
Foi ouvida a Comissão Nacional de Proteção de Dados, o ICP - Autoridade Nacional de Comunicações, o Banco de Portugal, a Comissão de Mercado de Valores Mobiliários, o Instituto de Seguros de Portugal, a Unidade de Missão Inovação e Conhecimento, o Instituto do Consumidor, a Associação Portuguesa para a Defesa dos Consumidores, a Associação Fonográfica Portuguesa e a Sociedade Portuguesa de Autores.

CAPÍTULO I
OBJETO E ÂMBITO

Artigo 1.º Objeto
O presente diploma transpõe para a ordem jurídica interna a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre Comércio Eletrónico) bem como o artigo 13.º da Diretiva n.º 2002/58/CE, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e a proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à Privacidade e às Comunicações Eletrónicas).

Artigo 2.º Âmbito
1. Estão fora do âmbito do presente diploma:
a) A matéria fiscal;

b) A disciplina da concorrência;

c) O regime do tratamento de dados pessoais e da proteção da privacidade;

d) O patrocínio judiciário;

e) Os jogos de fortuna, incluindo lotarias e apostas, em que é feita uma aposta em dinheiro;

f) A atividade notarial ou equiparadas, enquanto caracterizadas pela fé pública ou por outras manifestações de poderes públicos.

2. O presente diploma não afeta as medidas tomadas a nível comunitário ou nacional na observância do direito comunitário para fomentar a diversidade cultural e linguística e para assegurar o pluralismo.

CAPÍTULO II
PRESTADORES DE SERVIÇOS DA SOCIEDADE DA INFORMAÇÃO

Artigo 3.º Princípio da liberdade de exercício

1. Entende-se por «serviço da sociedade da informação» qualquer serviço prestado a distância por via eletrónica, mediante remuneração ou pelo menos no âmbito de uma atividade económica na sequência de pedido individual do destinatário.

2. Não são serviços da sociedade da informação os enumerados no anexo ao Decreto-Lei n.º 58/2000, de 18 de Abril, salvo no que respeita aos serviços contemplados nas alíneas c), d) e e) do n.º 1 daquele anexo.

3. A atividade de prestador de serviços da sociedade da informação não depende de autorização prévia.

4. Excetua-se o disposto no domínio das telecomunicações, bem como todo o regime de autorização que não vise especial e exclusivamente os serviços da sociedade da informação.

5. O disposto no presente diploma não exclui a aplicação da legislação vigente que com ele seja compatível, nomeadamente no que respeita

ao regime dos contratos celebrados a distância e não prejudica o nível de proteção dos consumidores, incluindo investidores, resultante da restante legislação nacional.

Artigo 4.º Prestadores de serviços estabelecidos em Portugal
1. Os prestadores de serviços da sociedade da informação estabelecidos em Portugal ficam integralmente sujeitos à lei portuguesa relativa à atividade que exercem, mesmo no que concerne a serviços da sociedade da informação prestados noutro país comunitário.
2. Um prestador de serviços que exerça uma atividade económica no país mediante um estabelecimento efetivo considera-se estabelecido em Portugal seja qual for a localização da sua sede, não configurando a mera disponibilidade de meios técnicos adequados à prestação do serviço, só por si, um estabelecimento efetivo.

3. O prestador estabelecido em vários locais considera-se estabelecido, para efeitos do n.º 1, no local em que tenha o centro das suas atividades relacionadas com o serviço da sociedade da informação.

4. Os prestadores intermediários de serviços em rede que pretendam exercer estavelmente a atividade em Portugal devem previamente proceder à inscrição junto da entidade de supervisão central.

5. «Prestadores intermediários de serviços em rede» são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço.

Artigo 5.º Livre prestação de serviços
1. Aos prestadores de serviços da sociedade da informação não estabelecidos em Portugal mas estabelecidos noutro Estado membro da União Europeia é aplicável, exclusivamente no que respeita a atividades em linha, a lei do lugar do estabelecimento:
a) Aos próprios prestadores, nomeadamente no que respeita a habilitações, autorizações e notificações, à identificação e à responsabilidade;

b) Ao exercício, nomeadamente no que respeita à qualidade e conteúdo dos serviços, à publicidade e aos contratos.

2. É livre a prestação dos serviços referidos no número anterior, com as limitações constantes dos artigos seguintes.

3. Os serviços de origem extracomunitária estão sujeitos à aplicação geral da lei portuguesa, ficando também sujeitos a este diploma em tudo o que não for justificado pela especificidade das relações intracomunitárias.

Artigo 6.º Exclusões
Estão fora do âmbito de aplicação dos artigos 4.º, n.º 1, e 5.º, n.º 1:
a) A propriedade intelectual, incluindo a proteção das bases de dados e das topografias dos produtos semicondutores;

b) A emissão de moeda eletrónica, por efeito de derrogação prevista no n.º 1 do artigo 8.º da Diretiva n.º 2000/46/CE;

c) A publicidade realizada por um organismo de investimento coletivo em valores mobiliários, nos termos do n.º 2 do artigo 44.º da Diretiva n.º 85/611/CEE;

d) A atividade seguradora, quanto a seguros obrigatórios, alcance e condições da autorização da entidade seguradora e empresas em dificuldades ou em situação irregular;

e) A matéria disciplinada por legislação escolhida pelas partes no uso da autonomia privada;

f) Os contratos celebrados com consumidores, no que respeita às obrigações deles emergentes;

g) A validade dos contratos em função da observância de requisitos legais de forma, em contratos relativos a direitos reais sobre imóveis;

h) A permissibilidade do envio de mensagens publicitárias não solicitadas por correio eletrónico.

Artigo 7.º Medidas restritivas
1. Podem ser adotadas medidas, incluindo providências concretas contra um prestador de serviços, restritivas à circulação de um determinado

serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente:
a) A dignidade humana ou a ordem pública, incluindo a proteção de menores e a repressão do incitamento ao ódio fundado na raça, no sexo, na religião ou na nacionalidade, nomeadamente por razões de prevenção ou repressão de crimes ou de ilícitos de mera ordenação social;

b) A saúde pública;

c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais;

d) Os consumidores, incluindo os investidores.

2. A adoção deve ser precedida:
a) Da solicitação ao Estado membro de origem do prestador do serviço que ponha cobro à situação;

b) Caso este o não tenha feito, ou as medidas que tome se revelem inadequadas, da notificação à Comissão e ao Estado membro de origem da intenção de adotar as medidas restritivas.

3. O disposto no número anterior não prejudica a realização de diligências judiciais, incluindo a instrução e demais atos praticados no âmbito de uma investigação criminal ou de um ilícito de mera ordenação social.

4. As medidas adotadas devem ser proporcionais aos objetivos a tutelar.

Artigo 8.º Atuação em caso de urgência
Em caso de urgência, as entidades competentes, incluindo os tribunais, podem tomar medidas restritivas não precedidas das notificações à Comissão e aos outros Estados membros de origem previstas no artigo anterior.

Artigo 9.º Comunicação à entidade de supervisão central
1. As entidades competentes que desejem promover a solicitação ao Estado membro de origem que ponha cobro a uma situação violadora

devem comunicá-lo à entidade de supervisão central, a fim de ser notificada ao Estado membro de origem.

2. As entidades competentes que tenham a intenção de tomar medidas restritivas, ou as tomem efetivamente, devem comunicá-lo imediatamente à autoridade de supervisão central, a fim de serem notificadas à Comissão e aos Estados membros de origem.

3. Tratando-se de medidas restritivas de urgência devem ser também indicadas as razões da urgência na sua adoção.

Artigo 10.º Disponibilização permanente de informações
1. Os prestadores de serviços devem disponibilizar permanentemente em linha, em condições que permitam um acesso fácil e direto, elementos completos de identificação que incluam, nomeadamente:
a) Nome ou denominação social;

b) Endereço geográfico em que se encontra estabelecido e endereço eletrónico, em termos de permitir uma comunicação direta;

c) Inscrições do prestador em registos públicos e respetivos números de registo;

d) Número de identificação fiscal.

2. Se o prestador exercer uma atividade sujeita a um regime de autorização prévia, deve disponibilizar a informação relativa à entidade que a concedeu.

3. Se o prestador exercer uma profissão regulamentada deve também indicar o título profissional e o Estado membro em que foi concedido, a entidade profissional em que se encontra inscrito, bem como referenciar as regras profissionais que disciplinam o acesso e o exercício dessa profissão.

4. Se os serviços prestados implicarem custos para os destinatários além dos custos dos serviços de telecomunicações, incluindo ónus fiscais ou despesas de entrega, estes devem ser objeto de informação clara anterior à utilização dos serviços.

CAPÍTULO III
RESPONSABILIDADE DOS PRESTADORES DE SERVIÇOS EM REDE

Artigo 11.º Princípio da equiparação
A responsabilidade dos prestadores de serviços em rede está sujeita ao regime comum, nomeadamente em caso de associação de conteúdos, com as especificações constantes dos artigos seguintes.

Artigo 12.º Ausência de um dever geral de vigilância dos prestadores intermediários de serviços
Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito.

Artigo 13.º Deveres comuns dos prestadores intermediários dos serviços
Cabe aos prestadores intermediários de serviços a obrigação para com as entidades competentes:
a) De informar de imediato quando tiverem conhecimento de atividades ilícitas que se desenvolvam por via dos serviços que prestam;

b) De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem;

c) De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infração, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação;

d) De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido.

Artigo 14.º Simples transporte
1. O prestador intermediário de serviços que prossiga apenas a atividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na seleção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas.

2. A irresponsabilidade mantém-se ainda que o prestador realize a armazenagem meramente tecnológica das informações no decurso do processo de transmissão, exclusivamente para as finalidades de transmissão e durante o tempo necessário para esta.

Artigo 15.º Armazenagem intermediária
1. O prestador intermediário de serviços de transmissão de comunicações em rede que não tenha intervenção no conteúdo das mensagens transmitidas nem na seleção destas ou dos destinatários e respeite as condições de acesso à informação é isento de toda a responsabilidade pela armazenagem temporária e automática, exclusivamente para tornar mais eficaz e económica a transmissão posterior a nova solicitação de destinatários do serviço.

2. Passa, porém, a aplicar-se o regime comum de responsabilidade se o prestador não proceder segundo as regras usuais do sector:
a) Na atualização da informação;

b) No uso da tecnologia, aproveitando-a para obter dados sobre a utilização da informação.

3. As regras comuns passam também a ser aplicáveis se chegar ao conhecimento do prestador que a informação foi retirada da fonte originária ou o acesso tornado impossível ou ainda que um tribunal ou entidade administrativa com competência sobre o prestador que está na origem da informação ordenou essa remoção ou impossibilidade de acesso com exequibilidade imediata e o prestador não a retirar ou impossibilitar imediatamente o acesso.

Artigo 16.º Armazenagem principal
1. O prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento de atividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação.

2. Há responsabilidade civil sempre que, perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação.

3. Aplicam-se as regras comuns de responsabilidade sempre que o destinatário do serviço atuar subordinado ao prestador ou for por ele controlado.

Artigo 17.º Responsabilidade dos prestadores intermediários de serviços de associação de conteúdos
Os prestadores intermediários de serviços de associação de conteúdos em rede, por meio de instrumentos de busca, hiperconexões ou processos análogos que permitam o acesso a conteúdos ilícitos estão sujeitos a regime de responsabilidade correspondente ao estabelecido no artigo anterior.

Artigo 18.º Solução provisória de litígios
1. Nos casos contemplados nos artigos 16.º e 17.º, o prestador intermediário de serviços, se a ilicitude não for manifesta, não é obrigado a remover o conteúdo contestado ou a impossibilitar o acesso à informação só pelo facto de um interessado arguir uma violação.

2. Nos casos previstos no número anterior, qualquer interessado pode recorrer à entidade de supervisão respetiva, que deve dar uma solução provisória em quarenta e oito horas e logo a comunica eletronicamente aos intervenientes.

3. Quem tiver interesse jurídico na manutenção daquele conteúdo em linha pode nos mesmos termos recorrer à entidade de supervisão contra uma decisão do prestador de remover ou impossibilitar o acesso a esse conteúdo, para obter a solução provisória do litígio.

4. O procedimento perante a entidade de supervisão será especialmente regulamentado.

5. A entidade de supervisão pode a qualquer tempo alterar a composição provisória do litígio estabelecida.

6. Qualquer que venha a ser a decisão, nenhuma responsabilidade recai sobre a entidade de supervisão e tão-pouco recai sobre o prestador intermediário de serviços por ter ou não retirado o conteúdo ou impossibilitado o acesso a mera solicitação, quando não for manifesto se há ou não ilicitude.

7. A solução definitiva do litígio é realizada nos termos e pelas vias comuns.

8. O recurso a estes meios não prejudica a utilização pelos interessados, mesmo simultânea, dos meios judiciais comuns.

Artigo 19.º Relação com o direito à informação
1. A associação de conteúdos não é considerada irregular unicamente por haver conteúdos ilícitos no sítio de destino, ainda que o prestador tenha consciência do facto.

2. A remissão é lícita se for realizada com objetividade e distanciamento, representando o exercício do direito à informação, sendo, pelo contrário, ilícita se representar uma maneira de tomar como próprio o conteúdo ilícito para que se remete.

3. A avaliação é realizada perante as circunstâncias do caso, nomeadamente:
a) A confusão eventual dos conteúdos do sítio de origem com os de destino;

b) O carácter automatizado ou intencional da remissão;

c) A área do sítio de destino para onde a remissão é efetuada.

CAPÍTULO IV
COMUNICAÇÕES PUBLICITÁRIAS EM REDE E MARKETING DIRETO

Artigo 20.º Âmbito
1. Não constituem comunicação publicitária em rede:
a) Mensagens que se limitem a identificar ou permitir o acesso a um operador económico ou identifiquem objetivamente bens, serviços ou a imagem de um operador, em coletâneas ou listas, particularmente quando não tiverem implicações financeiras, embora se integrem em serviços da sociedade da informação;

b) Mensagens destinadas a promover ideias, princípios, iniciativas ou instituições.

2. A comunicação publicitária pode ter somente por fim promover a

imagem de um operador comercial, industrial, artesanal ou integrante de uma profissão regulamentada.

Artigo 21.º Identificação e informação
Nas comunicações publicitárias prestadas à distância, por via eletrónica, devem ser claramente identificados de modo a serem apreendidos com facilidade por um destinatário comum:
a) A natureza publicitária, logo que a mensagem seja apresentada no terminal e de forma ostensiva;

b) O anunciante;

c) As ofertas promocionais, como descontos, prémios ou brindes, e os concursos ou jogos promocionais, bem como os condicionalismos a que ficam submetidos.

Artigo 22.º Comunicações não solicitadas
(Revogado)

Artigo 23.º Profissões regulamentadas
1. As comunicações publicitárias à distância por via eletrónica em profissões regulamentadas são permitidas na medida em que cumpram as regras deontológicas de cada profissão, relativas à independência, sigilo profissional e lealdade para com o público e membros da profissão entre si.

2. «Profissão regulamentada» é entendido no sentido constante dos diplomas relativos ao reconhecimento, na União Europeia, de formações profissionais.

CAPÍTULO V
CONTRATAÇÃO ELETRÓNICA

Artigo 24.º Âmbito
As disposições deste capítulo são aplicáveis a todo o tipo de contratos celebrados por via eletrónica ou informática, sejam ou não qualificáveis como comerciais.

Artigo 25.º Liberdade de celebração
1. É livre a celebração de contratos por via eletrónica, sem que a validade ou eficácia destes seja prejudicada pela utilização deste meio.

2. São excluídos do princípio da admissibilidade os negócios jurídicos:
a) Familiares e sucessórios;

b) Que exijam a intervenção de tribunais, entes públicos ou outros entes que exerçam poderes públicos, nomeadamente quando aquela intervenção condicione a produção de efeitos em relação a terceiros e ainda os negócios legalmente sujeitos a reconhecimento ou autenticação notariais;

c) Reais imobiliários, com exceção do arrendamento;

d) De caução e de garantia, quando não se integrarem na atividade profissional de quem as presta.

3. Só tem de aceitar a via eletrónica para a celebração de um contrato quem se tiver vinculado a proceder dessa forma.

4. São proibidas cláusulas contratuais gerais que imponham a celebração por via electrónica dos contratos com consumidores.

Artigo 26.º Forma
1. As declarações emitidas por via eletrónica satisfazem a exigência legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação.

2. O documento eletrónico vale como documento assinado quando satisfizer os requisitos da legislação sobre assinatura eletrónica e certificação.

Artigo 27.º Dispositivos de identificação e correção de erros
O prestador de serviços em rede que celebre contratos por via eletrónica deve disponibilizar aos destinatários dos serviços, salvo acordo em contrário das partes que não sejam consumidores, meios técnicos eficazes que lhes permitam identificar e corrigir erros de introdução, antes de formular uma ordem de encomenda.

Artigo 28.º Informações prévias
1. O prestador de serviços em rede que celebre contratos em linha deve facultar aos destinatários, antes de ser dada a ordem de encomenda, informação mínima inequívoca que inclua:
a) O processo de celebração do contrato;

b) O arquivamento ou não do contrato pelo prestador de serviço e a acessibilidade àquele pelo destinatário;

c) A língua ou línguas em que o contrato pode ser celebrado;

d) Os meios técnicos que o prestador disponibiliza para poderem ser identificados e corrigidos erros de introdução que possam estar contidos na ordem de encomenda;

e) Os termos contratuais e as cláusulas gerais do contrato a celebrar;

f) Os códigos de conduta de que seja subscritor e a forma de os consultar eletronicamente.

2. O disposto no número anterior é derrogável por acordo em contrário das partes que não sejam consumidores.

Artigo 29.º Ordem de encomenda e aviso de receção
1. Logo que receba uma ordem de encomenda por via exclusivamente eletrónica, o prestador de serviços deve acusar a receção igualmente por meios eletrónicos, salvo acordo em contrário com a parte que não seja consumidora.

2. É dispensado o aviso de receção da encomenda nos casos em que há a imediata prestação em linha do produto ou serviço.

3. O aviso de receção deve conter a identificação fundamental do contrato a que se refere.

4. O prestador satisfaz o dever de acusar a receção se enviar a comunicação para o endereço eletrónico que foi indicado ou utilizado pelo destinatário do serviço.

5. A encomenda torna-se definitiva com a confirmação do destinatário, dada na sequência do aviso de receção, reiterando a ordem emitida.

Artigo 30.º Contratos celebrados por meio de comunicação individual
Os artigos 27.º a 29.º não são aplicáveis aos contratos celebrados exclusivamente por correio eletrónico ou outro meio de comunicação individual equivalente.

Artigo 31.º Apresentação dos termos contratuais e cláusulas gerais
1. Os termos contratuais e as cláusulas gerais, bem como o aviso de receção, devem ser sempre comunicados de maneira que permita ao destinatário armazená-los e reproduzi-los.

2. A ordem de encomenda, o aviso de receção e a confirmação da encomenda consideram-se recebidos logo que os destinatários têm a possibilidade de aceder a eles.

Artigo 32.º Proposta contratual e convite a contratar
1. A oferta de produtos ou serviços em linha representa uma proposta contratual quando contiver todos os elementos necessários para que o contrato fique concluído com a simples aceitação do destinatário, representando, caso contrário, um convite a contratar.

2. O mero aviso de receção da ordem de encomenda não tem significado para a determinação do momento da conclusão do contrato.

Artigo 33.º Contratação sem intervenção humana
1. À contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, é aplicável o regime comum, salvo quando este pressupuser uma atuação.

2. São aplicáveis as disposições sobre erro:
a) Na formação da vontade, se houver erro de programação;

b) Na declaração, se houver defeito de funcionamento da máquina;

c) Na transmissão, se a mensagem chegar deformada ao seu destino.

3. A outra parte não pode opor-se à impugnação por erro sempre que lhe fosse exigível que dele se apercebesse, nomeadamente pelo uso de dispositivos de deteção de erros de introdução.

Artigo 34.º Solução de litígios por via eletrónica
É permitido o funcionamento em rede de formas de solução extrajudicial de litígios entre prestadores e destinatários de serviços da sociedade da informação, com observância das disposições concernentes à validade e eficácia dos documentos referidas no presente capítulo.

CAPÍTULO VI
ENTIDADES DE SUPERVISÃO E REGIME SANCIONATÓRIO

Artigo 35.º Entidade de supervisão central
1. É instituída uma entidade de supervisão central com atribuições em todos os domínios regulados pelo presente diploma, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade.

2. As funções de entidade de supervisão central serão exercidas pela ICP - Autoridade Nacional de Comunicações (ICP-ANACOM).

Artigo 36.º Atribuições e competência
1. As entidades de supervisão funcionam como organismos de referência para os contactos que se estabeleçam no seu domínio, fornecendo, quando requeridas, informações aos destinatários, aos prestadores de serviços e ao público em geral.

2. Cabe às entidades de supervisão, além das atribuições gerais já assinaladas e das que lhes forem especificamente atribuídas:
a) Adotar as medidas restritivas previstas nos artigos 7.º e 8.º;

b) Elaborar regulamentos e dar instruções sobre práticas a ser seguidas para cumprimento do disposto no presente diploma;

c) Fiscalizar o cumprimento do preceituado sobre o comércio eletrónico;

d) Instaurar e instruir processos contraordenacionais e, bem assim, aplicar as sanções previstas;

e) Determinar a suspensão da atividade dos prestadores de serviços em face de graves irregularidades e por razões de urgência.

3. A entidade de supervisão central tem competência em todas as matérias que a lei atribua a um órgão administrativo sem mais especificação e nas que lhe forem particularmente cometidas.

4. Cabe designadamente à entidade de supervisão central, além das atribuições gerais já assinaladas, quando não couberem a outro órgão:
a) Publicitar em rede os códigos de conduta mais significativos de que tenha conhecimento;

b) Publicitar outras informações, nomeadamente decisões judiciais neste domínio;

c) Promover as comunicações à Comissão Europeia e ao Estado membro de origem previstas no artigo 9.º;

d) Em geral, desempenhar a função de entidade permanente de contacto com os outros Estados membros e com a Comissão Europeia, sem prejuízo das competências que forem atribuídas a entidades sectoriais de supervisão.

Artigo 37.º Contraordenação
1. Constitui contraordenação sancionável com coima de € 2500 a € 50 000 a prática dos seguintes atos pelos prestadores de serviços:
a) A não disponibilização ou a prestação de informação aos destinatários regulada nos artigos 10.º, 13.º e 21.º e no n.º 1 do artigo 28.º;

b) *(Revogado)*

c) A não disponibilização aos destinatários, quando devido, de dispositivos de identificação e correção de erros de introdução, tal como previsto no artigo 27.º;

d) A omissão de pronto envio do aviso de receção da ordem de encomenda previsto no artigo 29.º;

e) A não comunicação dos termos contratuais, cláusulas gerais e avisos de receção previstos no artigo 31.º, de modo que permita aos destinatários armazená-los e reproduzi-los;

f) A não prestação de informações solicitadas pela entidade de supervisão.

2. Constitui contraordenação sancionável com coima de € 5000 a € 100 000 a prática dos seguintes atos pelos prestadores de serviços:
a) A desobediência a determinação da entidade de supervisão ou de outra entidade competente de identificar os destinatários dos serviços com quem tenham acordos de transmissão ou de armazenagem, tal como previsto na alínea b) do artigo 13.º;

b) O não cumprimento de determinação do tribunal ou da autoridade competente de prevenir ou pôr termo a uma infração nos termos da alínea c) do artigo 13.º;

c) A omissão de informação à autoridade competente sobre atividades ilícitas de que tenham conhecimento, praticadas por via dos serviços que prestam, tal como previsto na alínea a) do artigo 13.º;

d) A não remoção ou impedimento do acesso a informação que armazenem e cuja ilicitude manifesta seja do seu conhecimento, tal como previsto nos artigos 16.º e 17.º;

e) A não remoção ou impedimento do acesso a informação que armazenem, se, nos termos do artigo 15.º, n.º 3, tiverem conhecimento que foi retirada da fonte, ou o acesso tornado impossível, ou ainda que um tribunal ou autoridade administrativa da origem ordenou essa remoção ou impossibilidade de acesso para ter exequibilidade imediata;

f) A prática com reincidência das infrações previstas no n.º 1.

3. Constitui contraordenação sancionável com coima de € 2500 a € 100 000 a prestação de serviços de associação de conteúdos, nas condições da alínea e) do n.º 2, quando os prestadores de serviços não impossibilitem a localização ou o acesso a informação ilícita.

4. A negligência é sancionável nos limites da coima aplicável às infrações previstas no n.º 1.

5. A prática da infração por pessoa coletiva agrava em um terço os limites máximo e mínimo da coima.

Artigo 38.º Sanções acessórias
1. Às contraordenações acima previstas pode ser aplicada a sanção acessória de perda a favor do Estado dos bens usados para a prática das infrações.

2. Em função da gravidade da infração, da culpa do agente ou da prática reincidente das infrações, pode ser aplicada, simultaneamente com as coimas previstas no n.º 2 do artigo anterior, a sanção acessória de interdição do exercício da atividade pelo período máximo de seis anos e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação durante o mesmo período.

3. A aplicação de medidas acessórias de interdição do exercício da atividade e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação por prazo superior a dois anos será obrigatoriamente decidida judicialmente por iniciativa oficiosa da própria entidade de supervisão.

4. Pode dar-se adequada publicidade à punição por contraordenação, bem como às sanções acessórias aplicadas nos termos do presente diploma.

Artigo 39.º Providências provisórias
1. A entidade de supervisão a quem caiba a aplicação da coima pode determinar, desde que se revelem imediatamente necessárias, as seguintes providências provisórias:
a) A suspensão da atividade e o encerramento do estabelecimento que é suporte daqueles serviços da sociedade da informação, enquanto decorre o procedimento e até à decisão definitiva;

b) A apreensão de bens que sejam veículo da prática da infração.

2. Estas providências podem ser determinadas, modificadas ou levantadas em qualquer momento pela própria entidade de supervisão, por sua iniciativa ou a requerimento dos interessados e a sua legalidade pode ser impugnada em juízo.

Artigo 40.º Destino das coimas
O montante das coimas cobradas reverte para o Estado e para a entidade que as aplicou na proporção de 60% e 40%, respetivamente.

Artigo 41.º Regras aplicáveis
1. O regime sancionatório estabelecido não prejudica os regimes sancionatórios especiais vigentes.

2. A entidade competente para a instauração, instrução e aplicação das sanções é a entidade de supervisão central ou as sectoriais, consoante a natureza das matérias.

3. É aplicável subsidiariamente o regime geral das contraordenações.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Artigo 42.º Códigos de conduta
1. As entidades de supervisão estimularão a criação de códigos de conduta pelos interessados e sua difusão por estes por via eletrónica.

2. Será incentivada a participação das associações e organismos que têm a seu cargo os interesses dos consumidores na formulação e aplicação de códigos de conduta, sempre que estiverem em causa os interesses destes. Quando houver que considerar necessidades específicas de associações representativas de deficientes visuais ou outros, estas deverão ser consultadas.

3. Os códigos de conduta devem ser publicitados em rede pelas próprias entidades de supervisão.

Artigo 43.º Impugnação
As entidades de supervisão e o Ministério Público têm legitimidade

para impugnar em juízo os códigos de conduta aprovados em domínio abrangido por este diploma que extravasem das finalidades da entidade que os emitiu ou tenham conteúdo contrário a princípios gerais ou regras vigentes.

Visto e aprovado em Conselho de Ministros de 31 de Outubro de 2003.
José Manuel Durão Barroso - Maria Manuela Dias Ferreira Leite - Maria Teresa Pinto Basto Gouveia - Maria Celeste Ferreira Lopes Cardona - José Luís Fazenda Arnaut Duarte - Carlos Manuel Tavares da Silva - Maria da Graça Martins da Silva Carvalho.

Promulgado em 19 de Dezembro de 2003.
Publique-se.

O Presidente da República,
Jorge Sampaio.

Referendado em 23 de Dezembro de 2003.
O Primeiro-Ministro,
José Manuel Durão Barroso.

10. Diretiva 2000/31/CE, do Parlamento Europeu e do Conselho relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (˝Diretiva sobre o comércio eletrónico˜)[9]

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia e, nomeadamente, o n.º 2 do seu artigo 47.º e os seus artigos 55.º e 95.º,

Tendo em conta a proposta da Comissão[10],

Tendo em conta o parecer do Comité Económico e Social[11],

Deliberando nos termos do artigo 251.º do Tratado[12]

Considerando o seguinte:
1 // A União Europeia pretende estabelecer laços cada vez mais estreitos entre os Estados e os povos europeus, com o objetivo de garantir o progresso económico e social. Nos termos do n.º 2 do artigo 14.º do Tratado, o mercado interno compreende um espaço sem fronteiras internas, no qual é assegurada a livre circulação de mercadorias e serviços, bem como a liberdade de estabelecimento. O desenvolvimento dos serviços da sociedade da informação no espaço sem fronteiras internas é essencial para eliminar as barreiras que dividem os povos europeus.

2 // O desenvolvimento do comércio eletrónico na sociedade da informação faculta oportunidades importantes de emprego na Comunidade, particularmente nas pequenas e médias empresas, e irá estimular o crescimento económico e o investimento na inovação por parte das

---

[9] Última modificação legislativa: Diretiva n.º 2009/22/CE, de 23 de Abril do Parlamento Europeu e do Conselho, de 23 de Abril de 2009, relativa às ações inibitórias em matéria de proteção dos interesses dos consumidores.

[10] JO C 30 de 5.2.1999, p. 4.

[11] JO C 169 de 16.6.1999, p. 36.

[12] Parecer do Parlamento Europeu de 6 de Maio de 1999 (JO C 279 de 1.10.1999, p. 389), posição comum do Conselho de 28 de Fevereiro de 2000 e decisão do Parlamento Europeu de 4 de Maio de 2000 (ainda não publicada no Jornal Oficial).

empresas europeias e pode igualmente reforçar a competitividade da indústria europeia, contanto que a internet seja acessível a todos.

3 // A legislação comunitária e as características da ordem jurídica comunitária constituem um meio essencial para que os cidadãos e os operadores europeus possam beneficiar, plenamente e sem consideração de fronteiras, das oportunidades proporcionadas pelo comércio eletrónico. A presente diretiva tem por isso por objeto assegurar um elevado nível de integração da legislação comunitária, a fim de estabelecer um real espaço sem fronteiras internas para os serviços da sociedade da informação.

4 // É importante assegurar que o comércio eletrónico possa beneficiar inteiramente do mercado interno e que assim se obtenha, tal como com a Diretiva 89/552/CEE do Conselho, de 3 de Outubro de 1989, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros relativas ao exercício de atividades de radiodifusão televisiva[13], um alto nível de integração comunitária.

5 // O desenvolvimento dos serviços da sociedade da informação na Comunidade é entravado por um certo número de obstáculos legais ao bom funcionamento do mercado interno, os quais, pela sua natureza, podem tornar menos atraente o exercício da liberdade de estabelecimento e a livre prestação de serviços. Esses obstáculos advêm da divergência das legislações, bem como da insegurança jurídica dos regimes nacionais aplicáveis a esses serviços. Na falta de coordenação e de ajustamento das várias legislações nos domínios em causa, há obstáculos que podem ser justificados à luz da jurisprudência do Tribunal de Justiça das Comunidades Europeias. Existe insegurança jurídica quanto à extensão do controlo que cada Estado-Membro pode exercer sobre serviços provenientes de outro Estado-Membro.

6 // À luz dos objetivos comunitários, dos artigos 43.º e 49.º do Tratado e do direito comunitário derivado, estes obstáculos devem ser abolidos, através da coordenação de determinadas legislações nacionais e da

[13] JO L 298 de 17.10.1989, p. 23. Diretiva alterada pela Diretiva 97/36/CE do Parlamento Europeu e do Conselho (JO L 202 de 30.7.1997, p. 60).

clarificação, a nível comunitário, de certos conceitos legais, na medida do necessário ao bom funcionamento do mercado interno. A presente

diretiva, ao tratar apenas de certas questões específicas que levantam problemas ao mercado interno, é plenamente coerente com a necessidade de respeitar o princípio da subsidiariedade, tal como enunciado no artigo 5.º do Tratado.

7 // A fim de garantir a segurança jurídica e a confiança do consumidor, é essencial que a presente diretiva estabeleça um quadro geral claro, que abranja certos aspetos legais do comércio eletrónico no mercado interno.

8 // O objetivo da presente diretiva é criar um enquadramento legal destinado a assegurar a livre circulação dos serviços da sociedade da informação entre os Estados-Membros, e não harmonizar o domínio do direito penal, enquanto tal.

9 // A livre circulação dos serviços da sociedade da informação pode em muitos casos constituir um reflexo específico, no direito comunitário, de um princípio mais geral, designadamente o da liberdade de expressão, consagrado no n.º 1 do artigo 10.º da Convenção para a proteção dos Direitos do Homem e das liberdades fundamentais, ratificada por todos os Estados-Membros. Por esta razão, as diretivas que cobrem a prestação de serviços da sociedade da informação devem assegurar que essa atividade possa ser empreendida livremente, à luz daquele preceito, apenas se subordinando às restrições fixadas no n.º 2 daquele artigo e no n.º 1 do artigo 46.º do Tratado. A presente diretiva não tem por objetivo afetar as normas e princípios nacionais fundamentais respeitantes à liberdade de expressão.

10 // De acordo com o princípio da proporcionalidade, as medidas previstas na presente diretiva limitam-se ao mínimo estritamente necessário para alcançar o objetivo do correto funcionamento do mercado interno. Sempre que seja necessário intervir a nível comunitário, e a fim de garantir a existência de um espaço efetivamente isento de fronteiras internas no que diz respeito ao comércio eletrónico, a presente diretiva deve assegurar um alto nível de proteção dos

objetivos de interesse geral, em especial a proteção dos menores e da dignidade humana, a defesa do consumidor e a proteção da saúde pública. Nos termos do artigo 152.º do Tratado, a proteção da saúde é uma componente essencial das outras políticas da Comunidade.

11 // A presente diretiva não prejudica o nível de proteção, designadamente, da saúde pública e do consumidor, estabelecido por instrumentos comunitários; nomeadamente a Diretiva 93/13/CEE do Conselho, de 5 de Abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores[14] e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho, de 20 de Maio de 1997, relativa à proteção dos consumidores em matéria de contratos à distância[15] constituem um elemento essencial da proteção do consumidor em matéria contratual. Essas diretivas aplicam-se igualmente na sua integralidade aos serviços da sociedade da informação. Fazem igualmente parte desse acervo a Diretiva 84/450/CEE do Conselho, de 10 de Setembro de 1984, relativa à publicidade enganosa e comparativa[16], a Diretiva 87/102/CEE do Conselho, de 22 de Dezembro de 1986, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros relativas ao crédito ao consumo[17], a Diretiva 93/22/CEE do Conselho, de 10 de Maio de 1993, relativa aos serviços de investimento no domínio dos valores mobiliários[18], a Diretiva 90/314/CEE do Conselho, de 13 de Junho de 1990, relativa às viagens organizadas, férias organizadas e circuitos organizados[19], a Diretiva 98/6/CE do Parlamento Europeu e do Conselho, de 16 de Fevereiro de 1998, relativa à defesa dos consumidores em matéria de indicações dos preços dos produtos oferecidos aos consumidores[20], a Diretiva 92/59/CEE do Conselho, de 29 de Junho de 1992, relativa à segurança geral dos produtos[21], a Diretiva 94/47/CE

---

[14] JO L 95 de 21.4.1993, p. 29.

[15] JO L 144 de 4.6.1997, p. 19.

[16] JO L 250 de 19.9.1984, p. 17. Diretiva alterada pela Diretiva 97/55/CE do Parlamento Europeu e do Conselho (JO L 290 de 23.10.1997, p. 18).

[17] JO L 42 de 12.2.1987, p. 48. Diretiva com a última redação que lhe foi dada pela Diretiva 98/7/CE do Parlamento Europeu e do Conselho (JO L 101 de 1.4.1998, p. 17).

[18] JO L 141 de 11.6.1993, p. 27. Diretiva com a última redação que lhe foi dada pela Diretiva 97/9/CE do Parlamento Europeu e do Conselho (JO L 84 de 26.3.1997, p. 22).

[19] JO L 158 de 23.6.1990, p. 59.

[20] JO L 80 de 18.3.1998, p. 27.

[21] JO L 228 de 11.8.1992, p. 24.

do Parlamento Europeu e do Conselho, de 26 de Outubro de 1994, relativa à proteção dos adquirentes quanto a certos aspetos dos contratos de aquisição de um direito de utilização a tempo parcial de bens imóveis[22], a Diretiva 98/27/CE do Parlamento Europeu e do Conselho, de 19 de Maio de 1998, relativa às ações inibitórias em matéria de proteção dos interesses dos consumidores[23], a Diretiva 85/374/CEE do Conselho, de 25 de Julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos[24], a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho, de 25 de Maio de 1999, relativa a certos aspetos da venda de bens de consumo e garantias conexas[25], a futura diretiva do Parlamento Europeu e do Conselho relativa à comercialização à distância de serviços financeiros junto dos consumidores a Diretiva 92/28/CEE do Conselho, de 31 de Março de 1992, relativa à publicidade dos medicamentos para uso humano[26]. A presente diretiva deve ser aplicável sem prejuízo do disposto na Diretiva 98/43/CE do Parlamento Europeu e do Conselho, de 6 de Julho de 1998, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de publicidade e de patrocínio dos produtos do tabaco[27], que foi adotada no âmbito do mercado interno, e nas diretivas relativas à proteção da saúde pública. A presente diretiva é complementar dos requisitos de informação fixados nas diretivas citadas, e em especial na Diretiva 97/7/CE.

12 // É necessário excluir do âmbito de aplicação da presente diretiva certas atividades, tendo em conta que a livre circulação de serviços não pode, nesta fase, ser garantida ao abrigo do Tratado ou do direito comunitário derivado existente. Essa exclusão não deve contrariar eventuais instrumentos que possam ser necessários ao bom funcionamento do mercado interno. A tributação, especialmente

---

[22] JO L 280 de 29.10.1994, p. 83.

[23] JO L 166 de 11.6.1998, p. 51. Diretiva com a última redação que lhe foi dada pela Diretiva 1999/44/CE (JO L 171 de 7.7.1999, p. 12).

[24] JO L 210 de 7.8.1985, p. 29. Diretiva com a última redação que lhe foi dada pela Diretiva 1999/34/CE (JO L 141 de 4.6.1999, p. 20).

[25] JO L 171 de 7.7.1999, p. 12.

[26] JO L 113 de 30.4.1992, p. 13.

[27] JO L 213 de 30.7.1998, p. 9.

o imposto sobre o valor acrescentado aplicado a um grande número de serviços abrangidos pela presente diretiva, deve ser excluída do seu âmbito de aplicação.

13 // A presente diretiva não tem por objetivo fixar regras em matéria de obrigações fiscais, nem obstar à criação de instrumentos comunitários respeitantes aos aspetos fiscais do comércio eletrónico.

14 // A proteção dos indivíduos no que se refere ao tratamento dos dados pessoais é regida exclusivamente pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[28] e pela Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações[29], que se aplicam plenamente aos serviços da sociedade da informação. Essas diretivas criam já um quadro legal comunitário no domínio dos dados pessoais, pelo que não é necessário tratar essa questão na presente diretiva para garantir o bom funcionamento do mercado interno, em especial a livre circulação dos dados pessoais entre Estados-Membros. A execução e aplicação da presente diretiva deverão efetuar-se em absoluta conformidade com os princípios respeitantes à proteção dos dados pessoais, designadamente no que se refere às comunicações comerciais não solicitadas e à responsabilidade dos intermediários. A presente diretiva não pode impedir a utilização anónima de redes abertas, como, por exemplo, a internet.

15 // A confidencialidade das comunicações está assegurada pelo artigo 5.º da Diretiva 97/66/CE. Nos termos dessa diretiva, os Estados-Membros devem proibir qualquer forma de interceção ou de vigilância dessas comunicações, por pessoas que não sejam os remetentes ou os destinatários destas, exceto quando legalmente autorizados.

16 // A exclusão dos jogos de azar do âmbito de aplicação da presente diretiva apenas abrange os jogos de fortuna, lotarias e apostas

[28] *JO L 281 de 23.11.1995, p. 31.*

[29] *JO L 24 de 30.1.1998, p. 1.*

propriamente ditas, em que é feita uma aposta em dinheiro. Não se incluem os concursos ou jogos promocionais cujo objetivo seja fomentar a venda de mercadorias ou serviços e em que os prémios, quando os haja, sirvam apenas para adquirir as mercadorias ou serviços promovidos.

17 // Já existe uma definição de serviços da sociedade da informação na Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de Junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação[30] e na Diretiva 98/84/CE do Parlamento Europeu e do Conselho, de 20 de Novembro de 1998, relativa à proteção jurídica dos serviços que se baseiem ou consistam num acesso condicional[31]. Essa definição abrange qualquer serviço, em princípio pago à distância, por meio de equipamento eletrónico de processamento (incluindo a compressão digital) e o armazenamento de dados, e a pedido expresso do destinatário do serviço. Os serviços enumerados na lista indicativa do anexo V da Diretiva 98/34/CE que não envolvem tratamento e armazenamento de dados não são abrangidos por essa definição.

18 // Os serviços da sociedade da informação abrangem uma grande diversidade de atividades económicas. Tais atividades podem, nomeadamente, consistir na venda de mercadorias em linha. Não são abrangidas atividades como a entrega de mercadorias enquanto tal ou a prestação de serviços fora de linha. Os serviços da sociedade da informação não dão apenas a possibilidade de celebrar contratos em linha, mas também, tratando-se de uma atividade económica, serviços que não são remunerados pelo respetivo destinatário, como os que consistem em prestar informações em linha ou comunicações comerciais, ou ainda os que fornecem ferramentas de pesquisa, acesso e descarregamento de dados. Os serviços da sociedade da informação abrangem igualmente a transmissão de informação por meio de uma rede de comunicações, de fornecimento de acesso a uma rede de comunicações ou de armazenagem de informações prestadas por um destinatário do serviço. A radiodifusão televisiva, na aceção da Diretiva 89/552/CEE, e a radiodifusão não constituem serviços da sociedade

---

[30] JO L 204 de 21.7.1998, p. 37. Diretiva alterada pela Diretiva 98/48/CE (JO L 217 de 5.8.1998, p. 18).

[31] JO L 320 de 28.11.1998, p. 54.

da informação, dado não serem prestados mediante pedido individual. Ao invés, os serviços transmitidos ponto a ponto, como o vídeo a pedido ou o envio de comunicações comerciais por correio eletrónico são serviços da sociedade da informação. A utilização do correio eletrónico ou de comunicações comerciais equivalentes, por exemplo, por parte de pessoas singulares agindo fora da sua atividade comercial, empresarial ou profissional, incluindo a sua utilização para celebrar contratos entre essas pessoas, não são serviços da sociedade da informação. A relação contratual entre um assalariado e a sua entidade patronal não é um serviço da sociedade da informação. As atividades que, pela sua própria natureza, não podem ser exercidas à distância e por meios eletrónicos, tais como a revisão oficial de contas de sociedades, ou o aconselhamento médico, que exija o exame físico do doente, não são serviços da sociedade da informação.

19 // A determinação do local de estabelecimento do prestador deve fazer-se de acordo com a jurisprudência do Tribunal de Justiça, segundo a qual do conceito de estabelecimento é indissociável a prossecução efetiva de uma atividade económica, através de um estabelecimento fixo por um período indefinido. Este requisito encontra-se igualmente preenchido no caso de uma sociedade constituída por um período determinado. O local de estabelecimento, quando se trate de uma sociedade prestadora de serviços através de um sítio internet, não é o local onde se encontra a tecnologia de apoio a esse sítio ou o local em que este é acessível, mas sim o local em que essa sociedade desenvolve a sua atividade económica. Quando um prestador está estabelecido em vários locais, é importante determinar de que local de estabelecimento é prestado o serviço em questão. Em caso de dificuldade especial para determinar a partir de qual dos vários locais de estabelecimento é prestado o serviço em questão, considera-se que esse local é aquele em que o prestador tem o centro das suas atividades relacionadas com esse serviço específico.

20 // A definição de «destinatário de um serviço» abrange todos os tipos de utilização dos serviços da sociedade da informação, tanto por pessoas que prestem informações na internet como por pessoas que procuram informações na internet por razões privadas ou profissionais.

21 // O âmbito do domínio coordenado é definido sem prejuízo de futura harmonização comunitária em matéria de sociedade da informação e de futura legislação adotada a nível nacional conforme com o direito comunitário. O domínio coordenado abrange exclusivamente exigências respeitantes a atividades em linha, tais como a informação em linha, a publicidade em linha, as compras em linha e os contratos em linha, e não diz respeito aos requisitos legais exigidos pelos Estados-Membros em relação às mercadorias, tais como as normas de segurança, as obrigações de rotulagem ou a responsabilização pelos produtos, ou as exigências dos Estados-Membros respeitantes à entrega ou transporte de mercadorias, incluindo a distribuição de produtos medicinais. O domínio coordenado não abrange o exercício do direito de preempção por parte de entidades públicas relativamente a determinados bens, tais como obras de arte.

22 // O controlo dos serviços da sociedade da informação deve ser exercido na fonte da atividade, a fim de garantir uma proteção eficaz dos interesses gerais. Para isso, é necessário que a autoridade competente assegure essa proteção, não apenas aos cidadãos do seu país, mas também ao conjunto dos cidadãos da Comunidade. Para melhorar a confiança mútua entre Estados-Membros, é indispensável precisar claramente essa responsabilidade do Estado-Membro em que os serviços têm origem. Além disso, a fim de garantir a eficácia da livre circulação de serviços e a segurança jurídica para os prestadores e os destinatários, esses serviços devem estar sujeitos, em princípio, à legislação do Estado-Membro em que o prestador se encontra estabelecido.

23 // A presente diretiva não estabelece normas adicionais de direito internacional privado em matéria de conflitos de leis, nem abrange a jurisdição dos tribunais. O disposto na legislação aplicável por força das normas de conflitos do direito internacional privado não restringe a liberdade de prestar serviços da sociedade da informação nos termos constantes da presente diretiva.

24 // No contexto da presente diretiva, e não obstante a regra do controlo na origem dos serviços da sociedade da informação, é legítimo que, nas condições fixadas na presente diretiva, os Estados-Membros possam adotar medidas destinadas a restringir a livre circulação dos serviços da sociedade da informação.

25 // Os tribunais nacionais, incluindo os tribunais cíveis, competentes para conhecer dos litígios de direito privado, podem tomar medidas que constituam uma derrogação à liberdade de prestação de serviços da sociedade da informação de acordo com as condições constantes da presente diretiva.

26 // Os Estados-Membros, de acordo com as condições fixadas na presente diretiva, podem aplicar as suas legislações em matéria de direito penal e de direito processual penal para efeitos das diligências de investigação e outras medidas necessárias à deteção e incriminação de delitos penais, sem terem de notificar essas medidas à Comissão.

27 // A presente diretiva, juntamente com a futura diretiva do Parlamento Europeu e do Conselho relativa à comercialização à distância de serviços financeiros junto dos consumidores, contribui para criar um enquadramento legal para a prestação de serviços financeiros em linha. A presente diretiva não prejudica futuras iniciativas no domínio dos serviços financeiros, em especial no que diz respeito à harmonização das regras de conduta neste domínio. A faculdade conferida pela presente diretiva aos Estados-Membros de, em certas circunstâncias, restringirem a liberdade de prestação de serviços da sociedade da informação, por forma a proteger os consumidores, abrange igualmente medidas no domínio dos serviços financeiros, em especial medidas destinadas a proteger os investidores.

28 // A obrigação dos Estados-Membros de não sujeitarem o acesso à atividade de prestador de serviços da sociedade da informação a autorização prévia não abrange os serviços postais, cobertos pela Diretiva 97/67/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa às regras comuns para o desenvolvimento do mercado interno dos serviços postais comunitários e a melhoria da qualidade de serviço[32], que consistam na entrega física de uma mensagem de correio eletrónico impressa e não afeta os sistemas de acreditação voluntários, em especial em relação aos prestadores de serviços de certificação de assinaturas eletrónicas.

[32] *JO L 15 de 21.1.1998, p. 14.*

29 // A comunicação comercial é essencial para o financiamento dos serviços da sociedade da informação e para o desenvolvimento de uma grande variedade de novos serviços gratuitos. No interesse dos consumidores e da lealdade das transações, a comunicação comercial, incluindo descontos, ofertas e jogos promocionais, deve respeitar um certo número de obrigações relativas à transparência. Estes requisitos aplicam-se sem prejuízo do disposto na Diretiva 97/7/CE. A presente diretiva não afeta as diretivas existentes relativas às comunicações comerciais, em especial a Diretiva 98/43/CE.

30 // A transmissão de comunicações comerciais não solicitadas por correio eletrónico pode ser inconveniente para os consumidores e para os prestadores de serviços da sociedade da informação e perturbar o bom funcionamento das redes interativas. A questão do consentimento dos destinatários em relação a determinadas formas de comunicações comerciais não solicitadas não é abordada na presente diretiva, mas foi já abordada, em particular, na Diretiva 97/7/CE e na Diretiva 97/66/CE. Nos Estados-Membros que autorizem esse tipo de comunicações, deveriam ser incentivadas e facilitadas iniciativas de colocação de «filtros» por parte das empresas. Além disso, é necessário, em qualquer caso, que as comunicações comerciais não solicitadas sejam claramente identificáveis enquanto tal, por forma a melhorar a transparência e facilitar o funcionamento dessas iniciativas da indústria. As comunicações comerciais não solicitadas por correio eletrónico não devem implicar custos adicionais para o destinatário.

31 // Os Estados-Membros que permitam a comunicação comercial não solicitada por correio eletrónico por parte de um prestador estabelecido no seu território sem autorização prévia do destinatário têm de assegurar que o prestador consulta regularmente e respeita os registos de opção negativa («opt-out») onde se podem inscrever as pessoas singulares que não desejem receber esse tipo de comunicações.

32 // Para suprimir os entraves ao desenvolvimento dos serviços transfronteiriços na Comunidade que os membros das profissões regulamentadas poderiam propor na internet, é necessário garantir, a nível comunitário, o cumprimento das regras profissionais previstas para proteger, nomeadamente, o consumidor ou a saúde pública. Os

códigos de conduta a nível comunitário constituem a melhor forma para determinar as regras deontológicas aplicáveis à comunicação comercial e é necessário incentivar a sua elaboração, ou a sua eventual adaptação, sem prejuízo da autonomia dos organismos e associações profissionais.

33 // A presente diretiva complementa o direito comunitário e as legislações nacionais relativas às profissões regulamentadas, assegurando um conjunto coerente de regras aplicáveis neste domínio.

34 // Cada Estado-Membro ajustará a sua legislação relativa a requisitos, nomeadamente de forma, suscetíveis de dificultar o recurso a contratos por via eletrónica. O exame das legislações que necessitem deste ajustamento deve ser sistemático e abranger todas as etapas e atos necessários ao processo contratual, incluindo a celebração do contrato. Esse ajustamento deve ter como resultado tornar exequíveis os contratos celebrados por via eletrónica. O efeito legal das assinaturas eletrónicas é objeto da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para assinaturas eletrónicas[33]. O aviso de receção por parte de um prestador de serviços pode revestir a forma da prestação em linha do serviço pago.

35 // A presente diretiva não afeta a possibilidade de os Estados-Membros manterem ou fixarem requisitos legais, gerais ou específicos para os contratos, que possam ser preenchidos por meios eletrónicos, em especial os requisitos relativos à certificação de assinaturas eletrónicas.

36 // Os Estados-Membros podem manter restrições à celebração de contratos por meios eletrónicos quando estes exijam, por lei, a intervenção de tribunais, entidades públicas ou profissões que exercem poderes públicos. Essa possibilidade abrange igualmente os contratos que exijam a intervenção de tribunais, entidades públicas ou profissões que exercem poderes públicos para que possam produzir efeitos em relação a terceiros; bem como os contratos legalmente sujeitos a reconhecimento ou autenticação notariais.

37 // A obrigação de os Estados-Membros não colocarem obstáculos à celebração de contratos por meios eletrónicos apenas diz respeito

[33] *JO L 13 de 19.1.2000, p. 12.*

aos resultantes de requisitos legais, e não aos obstáculos práticos resultantes da impossibilidade de utilizar meios eletrónicos em determinados casos.

38 // A obrigação de os Estados-Membros não colocarem obstáculos à celebração de contratos por meios eletrónicos será aplicada de acordo com as exigências legais aplicáveis aos contratos consagradas no direito comunitário.

39 // As exceções às disposições relativas aos contratos celebrados exclusivamente por correio eletrónico, ou outro meio de comunicação individual equivalente, previsto na presente diretiva, no tocante às informações a prestar e às ordens de encomenda, não devem dar lugar a que os prestadores de serviços da sociedade da informação possam contornar as referidas disposições.

40 // As divergências atuais ou futuras, entre as legislações e jurisprudências nacionais no domínio da responsabilidade dos prestadores de serviços agindo na qualidade de intermediários, impedem o bom funcionamento do mercado interno, perturbando particularmente o desenvolvimento dos serviços transfronteiriços e produzindo distorções de concorrência. Os prestadores de serviços têm, em certos casos, o dever de agir a fim de evitar ou fazer cessar atividades ilícitas. A presente diretiva deve constituir a base adequada para a criação de mecanismos rápidos e fiáveis para remover as informações ilícitas e impossibilitar o acesso a estas. Esses mecanismos poderão ser elaborados com base em acordos voluntários negociados entre todas as partes interessadas e deveriam ser encorajados pelos Estados-Membros. É do interesse de todas as partes que participam na prestação de serviços da sociedade da informação adotar e aplicar esses mecanismos. As disposições da presente diretiva relativas à responsabilidade não deveriam constituir obstáculo ao desenvolvimento e aplicação efetiva, pelas diferentes partes envolvidas, de sistemas técnicos de proteção e identificação, bem como de instrumentos de controlo técnico, que a tecnologia digital permite, dentro dos limites previstos pelas Diretivas 95/46/CE e 97/66/CE.

41 // A presente diretiva estabelece um justo equilíbrio entre os diferentes interesses em jogo e consagra princípios em que se podem basear os acordos e normas da indústria.

42 // As isenções da responsabilidade estabelecidas na presente diretiva abrangem exclusivamente os casos em que a atividade da sociedade da informação exercida pelo prestador de serviços se limita ao processo técnico de exploração e abertura do acesso a uma rede de comunicação na qual as informações prestadas por terceiros são transmitidas ou temporariamente armazenadas com o propósito exclusivo de tornar a transmissão mais eficaz. Tal atividade é puramente técnica, automática e de natureza passiva, o que implica que o prestador de serviços da sociedade da informação não tem conhecimento da informação transmitida ou armazenada, nem o controlo desta.

43 // Um prestador pode beneficiar de isenções por simples transporte ou armazenagem temporária («caching») quando é inteiramente alheio à informação transmitida. Isso exige, designadamente, que o prestador não altere a informação que transmite. Esta exigência não se aplica ao manuseamento técnico que tem lugar no decurso da transmissão, uma vez que este não afeta a integridade da informação contida na transmissão.

44 // Um prestador que colabora deliberadamente com um dos destinatários do serviço prestado, com o intuito de praticar atos ilegais, ultrapassa as atividades de simples transporte ou armazenagem temporária («caching»), pelo que não pode beneficiar das isenções de responsabilidade aplicáveis a tais atividades.

45 // A delimitação da responsabilidade dos prestadores intermediários de serviços, fixada na presente diretiva, não afeta a possibilidade de medidas inibitórias de diversa natureza. Essas medidas podem consistir, designadamente, em decisões judiciais ou administrativas que exijam a prevenção ou a cessação de uma eventual infração, incluindo a remoção de informações ilegais, ou tornando impossível o acesso a estas.

46 // A fim de beneficiar de uma delimitação de responsabilidade, o prestador de um serviço da sociedade da informação, que consista na armazenagem de informação, a partir do momento em que tenha conhecimento efetivo da ilicitude, ou tenha sido alertado para esta, deve proceder com diligência no sentido de remover as informações ou impossibilitar o acesso a estas. A remoção ou impossibilitação de acesso

têm de ser efetuadas respeitando o princípio da liberdade de expressão. A presente diretiva não afeta a possibilidade de os Estados-Membros fixarem requisitos específicos que tenham de ser cumpridos de forma expedita, previamente à remoção ou à impossibilitação de acesso à informação.

47 // Os Estados-Membros só estão impedidos de impor uma obrigação de vigilância obrigatória dos prestadores de serviços em relação a obrigações de natureza geral. Esse impedimento não diz respeito a obrigações de vigilância em casos específicos e, em especial, não afeta as decisões das autoridades nacionais nos termos das legislações nacionais.

48 // A presente diretiva não afeta a possibilidade de os Estados-Membros exigirem dos prestadores de serviços, que acolham informações prestadas por destinatários dos seus serviços, que exerçam deveres de diligência que podem razoavelmente esperar-se deles e que estejam especificados na legislação nacional, no sentido de detetarem e prevenirem determinados tipos de atividades ilegais.

49 // Os Estados-Membros e a Comissão deverão incentivar a elaboração de códigos de conduta. Tal facto não deverá alterar o carácter voluntário desses códigos e a possibilidade de as partes interessadas decidirem livremente se aderem ou não a esses códigos.

50 // Importa que a proposta de diretiva relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação entre em vigor em prazo similar ao da presente diretiva, a fim de se estabelecer um conjunto de regras claro no que diz respeito à questão da responsabilidade dos intermediários pelas infrações aos direitos de autor e aos direitos conexos a nível comunitário.

51 // Deve caber a cada Estado-Membro, quando necessário, ajustar a sua legislação suscetível de dificultar a utilização dos mecanismos de resolução extrajudicial de litígios pelas vias eletrónicas apropriadas. Esse ajustamento deve ter como resultado tornar real e efetivamente possível, na lei e na prática, o funcionamento desses mecanismos, inclusive em situações transfronteiriças.

52 // O exercício efetivo das liberdades do mercado interno exige que se garanta às vítimas um acesso eficaz aos mecanismos de resolução de litígios. Os prejuízos que podem ocorrer no quadro dos serviços da sociedade da informação caracterizam-se pela rapidez e pela extensão geográfica. Em virtude desta especificidade e da necessidade de zelar por que as autoridades nacionais não ponham em causa a confiança mútua que devem ter, a presente diretiva requer dos Estados-Membros que assegurem a existência de meios de recurso judicial adequados. Os Estados-Membros devem estudar a necessidade de acesso a procedimentos judiciais por meios eletrónicos adequados.

53 // A Diretiva 98/27/CE, que é aplicável aos serviços da sociedade da informação, prevê um mecanismo para as ações inibitórias em matéria de proteção dos interesses coletivos dos consumidores. Esse mecanismo contribuirá para a livre circulação dos serviços da sociedade da informação, ao assegurar um elevado nível de proteção dos consumidores.

54 // As sanções previstas na presente diretiva não prejudicam qualquer outra penalidade ou medida prevista no direito interno. Os Estados-Membros não são obrigados a sancionar penalmente as infrações às normas nacionais adotadas em cumprimento da presente diretiva.

55 // A presente diretiva não afeta a legislação aplicável às obrigações contratuais relativas aos contratos celebrados pelos consumidores. Assim, a presente diretiva não pode ter como resultado privar o consumidor da proteção que lhe é concedida pelas disposições compulsivas relativas às obrigações contratuais, constantes da legislação do Estado-Membro em que este tem a sua residência habitual.

56 // No que se refere à derrogação prevista na presente diretiva relativa às obrigações contratuais relativas aos contratos celebrados pelos consumidores, estas devem ser interpretadas como abrangendo as informações sobre os elementos essenciais do contrato, incluindo os direitos do consumidor, que têm uma influência determinante na decisão de contratar.

57 // O Tribunal de Justiça tem sustentado de modo constante que um Estado-Membro mantém o direito de tomar medidas contra um prestador de serviços estabelecido noutro Estado-Membro, mas que dirige toda ou

a maior parte das suas atividades para o território do primeiro Estado-Membro, se a escolha do estabelecimento foi feita no intuito de iludir a legislação que se aplicaria ao prestador caso este se tivesse estabelecido no território desse primeiro Estado-Membro.

58 // A presente diretiva não deve aplicar-se aos serviços provenientes de prestadores estabelecidos em países terceiros. Dada a dimensão mundial do comércio eletrónico, deve, no entanto, ser garantida a coerência do quadro comunitário com o quadro internacional. A presente diretiva não prejudica os resultados das discussões que estão a decorrer no âmbito de organizações internacionais (nomeadamente, OMC, OCDE, CNUDCI) sobre os aspetos legais desta problemática.

59 // Apesar da natureza mundial das comunicações eletrónicas, é necessário coordenar as medidas reguladoras nacionais a nível da União Europeia, a fim de evitar a fragmentação do mercado interno e estabelecer um quadro regulamentar europeu apropriado. Essa coordenação deveria igualmente contribuir para criar uma posição negocial comum forte nos fóruns internacionais.

60 // Para facilitar o desenvolvimento sem entraves do comércio eletrónico, o quadro jurídico em questão deve ser simples, sóbrio, previsível e compatível com as regras em vigor a nível internacional, de modo a não prejudicar a competitividade da indústria europeia, nem impedir as ações inovadoras no sector.

61 // O efetivo funcionamento do mercado por via eletrónica num contexto mundializado exige a concertação entre a União Europeia e os grandes espaços não europeus para compatibilizar legislações e procedimentos.

62 // Deverá ser reforçada no sector do comércio eletrónico a cooperação com países terceiros, nomeadamente com os países candidatos à adesão e com os principais parceiros comerciais da União Europeia.

63 // A adoção da presente diretiva não impedirá os Estados-Membros de tomarem em conta as diversas implicações sociais, societais e culturais inerentes ao advento da sociedade da informação. Em especial, não deverá prejudicar as medidas que os Estados-Membros possam vir a adotar, de acordo com o direito comunitário, a fim de prosseguirem

objetivos sociais, culturais e democráticos que tenham em conta a sua diversidade linguística, as especificidades nacionais e regionais, bem como os respetivos patrimónios culturais, e para garantirem e preservarem o acesso público ao maior leque possível de serviços da sociedade da informação. O desenvolvimento da sociedade da informação deverá garantir, em qualquer caso, o acesso dos cidadãos europeus ao património cultural europeu facultado por meios digitais.

64 // Os Estados-Membros têm na comunicação eletrónica uma excelente via para a prestação de serviços públicos nas áreas cultural, educativa e linguística.

65 // O Conselho de Ministros, na sua resolução, de 19 de Janeiro de 1999, sobre os aspetos relativos ao consumidor na sociedade da informação[34], salientou que a defesa dos consumidores merecia uma atenção especial neste domínio. A Comissão irá analisar em que medida as regras de defesa do consumidor existentes facultam uma proteção adequada no contexto da sociedade da informação, identificando, quando necessário, as possíveis lacunas dessa legislação e os aspetos em relação aos quais poderão vir a ser necessárias medidas adicionais. Se necessário, a Comissão deverá apresentar propostas específicas adicionais destinadas a preencher as lacunas assim identificadas,

ADOTARAM A PRESENTE DIRECTIVA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º Objetivo e âmbito de aplicação
1. A presente diretiva tem por objetivo contribuir para o correto funcionamento do mercado interno, garantindo a livre circulação dos serviços da sociedade da informação entre Estados-Membros.

2. A presente diretiva aproxima, na medida do necessário à realização do objetivo previsto no n.º 1, certas disposições nacionais aplicáveis aos serviços da sociedade da informação que dizem respeito ao mercado interno, ao estabelecimento dos prestadores de serviços, às comunicações

[34] JO C 23 de 28.1.1999, p. 1.

comerciais, aos contratos celebrados por via eletrónica, à responsabilidade dos intermediários, aos códigos de conduta, à resolução extrajudicial de litígios, às ações judiciais e à cooperação entre Estados-Membros.

3. A presente diretiva é complementar da legislação comunitária aplicável aos serviços da sociedade da informação, sem prejuízo do nível de proteção, designadamente da saúde pública e dos interesses dos consumidores, tal como consta dos atos comunitários e da legislação nacional de aplicação destes, na medida em que não restrinjam a liberdade de prestação de serviços da sociedade da informação.

4. A presente diretiva não estabelece normas adicionais de direito internacional privado, nem abrange a jurisdição dos tribunais.

5. A presente diretiva não é aplicável:
a) Ao domínio tributário;

b) À questões respeitantes aos serviços da sociedade da informação abrangidas pelas Diretivas 95/46/CE e 97/66/CE;

c) Às questões relativas a acordos ou práticas regidas pela legislação sobre cartéis;

d) Às seguintes atividades do âmbito dos serviços da sociedade da informação:
- atividades dos notários ou profissões equivalentes, na medida em que se encontrem direta e especificamente ligadas ao exercício de poderes públicos,
- representação de um cliente e a defesa dos seus interesses em tribunal,
- jogos de azar em que é feita uma aposta em dinheiro em jogos de fortuna, incluindo lotarias e apostas.

6. A presente diretiva não afeta as medidas tomadas a nível comunitário ou nacional, na observância do direito comunitário, para fomentar a diversidade cultural e linguística e para assegurar o pluralismo.

Artigo 2.º Definições
Para efeitos da presente diretiva, entende-se por:

a) «Serviços da sociedade da informação»: os serviços da sociedade da informação na aceção do n.º 2 do artigo 1.º da Diretiva 83/34/CEE, alterada pela Diretiva 98/48/CE;

b) «Prestador de serviços»: qualquer pessoa, singular ou coletiva, que preste um serviço do âmbito da sociedade da informação;

c) «Prestador de serviços estabelecido»: o prestador que efetivamente exerça uma atividade económica através de uma instalação fixa, por um período indefinido. A presença e a utilização de meios técnicos e de tecnologias necessários para prestar o serviço não constituem, em si mesmos, o estabelecimento do prestador;

d) «Destinatário do serviço»: qualquer pessoa, singular ou coletiva, que, para fins profissionais ou não, utilize um serviço da sociedade da informação, nomeadamente para procurar ou para tornar acessível determinada informação;

e) «Consumidor»: qualquer pessoa singular que atue para fins alheios à sua atividade comercial, empresarial ou profissional;

f) «Comunicação comercial»: todas as formas de comunicação destinadas a promover, direta ou indiretamente, mercadorias, serviços ou a imagem de uma empresa, organização ou pessoa que exerça uma profissão regulamentada ou uma atividade de comércio, indústria ou artesanato.

Não constituem comunicações comerciais:
- as informações que permitam o acesso direto à atividade da sociedade, da organização ou da pessoa, nomeadamente um nome de área ou um endereço de correio eletrónico,
- as comunicações relativas às mercadorias, aos serviços ou à imagem da sociedade, organização ou pessoa, compiladas de forma imparcial, em particular quando não existam implicações financeiras;

g) «Atividades profissionais regulamentadas»: quaisquer atividades profissionais na aceção da alínea d) do artigo 1.º da Diretiva 89/48/CEE do Conselho, de 21 de Dezembro de 1988, relativa a um sistema geral de reconhecimento dos diplomas de ensino superior que sancionam

formações profissionais com uma duração mínima de três anos[35], ou de alínea f) do artigo 1.º da Diretiva 92/51/CEE do Conselho, de 18 de Junho de 1992, relativo a um segundo sistema geral de reconhecimento das formações profissionais, que completa a Diretiva 89/48/CEE[36];

h) «Domínio coordenado»: as exigências fixadas na legislação dos Estados-Membros, aplicáveis aos prestadores de serviços da sociedade da informação e aos serviços da sociedade da informação, independentemente de serem de natureza geral ou especificamente concebidos para esses prestadores e serviços:

i) O domínio coordenado diz respeito às exigências que o prestador de serviços tem de observar, no que se refere:
- ao exercício de atividades de um serviço da sociedade da informação, tal como os requisitos respeitantes às habilitações, autorizações e notificações,
- à prossecução de atividade de um serviço da sociedade da informação, tal como os requisitos respeitantes ao comportamento do prestador de serviços, à qualidade ou conteúdo do serviço, incluindo as aplicáveis à publicidade e aos contratos, ou as respeitantes à responsabilidade do prestador de serviços;

ii) O domínio coordenado não abrange exigências tais como as aplicáveis:
- às mercadorias, enquanto tais,
- à entrega de mercadorias,
- aos serviços não prestados por meios eletrónicos.

Artigo 3.º Mercado interno
1. Cada Estado-Membro assegurará que os serviços da sociedade da informação prestados por um prestador estabelecido no seu território

cumpram as disposições nacionais aplicáveis nesse Estado-Membro que se integrem no domínio coordenado.

---

[35] JO L 19 de 24.1.1989, p. 16.
[36] JO L 209 de 24.7.1992, p. 25. Diretiva com a última redação que lhe foi dada pela Diretiva 97/38/CE (JO L 184 de 12.7.1997, p. 31).

2. Os Estados-Membros não podem, por razões que relevem do domínio coordenado, restringir a livre circulação dos serviços da sociedade da informação provenientes de outro Estado-Membro.

3. Os n.os 1 e 2 não se aplicam aos domínios a que se refere o anexo.

4. Os Estados-Membros podem tomar medidas derrogatórias do n.º 2 em relação a determinado serviço da sociedade da informação, caso sejam preenchidas as seguintes condições:
a) As medidas devem ser:
i) Necessárias por uma das seguintes razões:
- defesa da ordem pública, em especial prevenção, investigação, deteção e incriminação de delitos penais, incluindo a proteção de menores e a luta contra o incitamento ao ódio fundado na raça, no sexo, na religião ou na nacionalidade, e contra as violações da dignidade humana de pessoas individuais,
- proteção da saúde pública,
- segurança pública, incluindo a salvaguarda da segurança e da defesa nacionais,
- defesa dos consumidores, incluindo os investidores;

ii) Tomadas relativamente a um determinado serviço da sociedade da informação que lese os objetivos referidos na subalínea i), ou que comporte um risco sério e grave de prejudicar esses objetivos;
iii) Proporcionais a esses objetivos;
b) Previamente à tomada das medidas em questão, e sem prejuízo de diligências judiciais, incluindo a instrução e os atos praticados no âmbito de uma investigação criminal, o Estado-Membro deve:
- ter solicitado ao Estado-Membro a que se refere o n.º 1 que tome medidas, sem que este último as tenha tomado ou se estas se tiverem revelado inadequadas,
- ter notificado à Comissão e ao Estado-Membro a que se refere o n.º 1 a sua intenção de tomar tais medidas.

5. Os Estados-Membros podem, em caso de urgência, derrogar às condições previstas na alínea b) do n.º 4. Nesse caso, as medidas devem ser notificadas no mais curto prazo à Comissão e ao Estado-Membro a que se refere o n.º 1, indicando as razões pelas quais consideram que existe uma situação de urgência.

6. Sem prejuízo da faculdade de o Estado-Membro prosseguir a aplicação das medidas em questão, a Comissão analisará, com a maior celeridade, a compatibilidade das medidas notificadas com o direito comunitário; se concluir que a medida é incompatível com o direito comunitário, a Comissão solicitará ao Estado-Membro em causa que se abstenha de tomar quaisquer outras medidas previstas, ou ponha termo, com urgência, às medidas já tomadas.

CAPÍTULO II
PRINCÍPIOS

SECÇÃO 1
REGIME DE ESTABELECIMENTO E DE INFORMAÇÃO

Artigo 4.º Princípio de não autorização prévia

1. Os Estados-Membros assegurarão que o exercício e a prossecução da atividade de prestador de serviços da sociedade da informação não podem estar sujeitas a autorização prévia ou a qualquer outro requisito de efeito equivalente.

2. O n.º 1 não afeta os regimes de autorização que não visem especial e exclusivamente os serviços da sociedade da informação, nem os regimes de autorização abrangidos pela Diretiva 97/13/CE do Parlamento Europeu e do Conselho, de 10 de Abril de 1997, relativa a um quadro comum para autorizações gerais e licenças individuais no domínio dos serviços de telecomunicações[37].

Artigo 5.º Informações gerais a prestar

1. Além de outros requisitos de informação constantes do direito comunitário, os Estados-Membros assegurarão que o prestador do serviço faculte aos destinatários do seu serviço e às autoridades

competentes um acesso fácil, direto e permanente, pelo menos, às seguintes informações:

a) Nome do prestador;

b) Endereço geográfico em que o prestador se encontra estabelecido;

c) Elementos de informação relativos ao prestador de serviços, incluindo

[37] *JO L 117 de 7.5.1997, p. 15.*

o seu endereço eletrónico, que permitam contactá-lo rapidamente e comunicar direta e efetivamente com ele;

d) Caso o prestador de serviços esteja inscrito numa conservatória de registo comercial ou num registo público equivalente, a identificação dessa conservatória e o número de registo do prestador de serviços, ou meios equivalentes de o identificar nesse registo;

e) Caso determinada atividade esteja sujeita a um regime de autorização, os elementos de informação relativos à autoridade de controlo competente;

f) No que respeita às profissões regulamentadas:
- organização profissional ou associações semelhantes em que o prestador esteja inscrito,
- título profissional e Estado-Membro em que foi concedido,
- a citação das regras profissionais aplicáveis no Estado-Membro de estabelecimento e dos meios de aceder a essas profissões;

g) Caso o prestador exerça uma atividade sujeita a IVA, o número de identificação a que se refere o n.º 1 do artigo 22.º da sexta Diretiva 77/388/CEE do Conselho, de 17 de Maio de 1977, relativa à harmonização das legislações dos Estados-Membros respeitantes aos impostos sobre o volume de negócios - sistema comum do imposto sobre o valor acrescentado: matéria coletável uniforme[38].

2. Além de outros requisitos de informação constantes da legislação comunitária, os Estados-Membros assegurarão que, no mínimo, sempre que os serviços da sociedade da informação indiquem preços, essa indicação seja clara e inequívoca e explicite obrigatoriamente se inclui quaisquer despesas fiscais e de entrega.

SECÇÃO 2
COMUNICAÇÕES COMERCIAIS

Artigo 6.º Informações a prestar
Além de outros requisitos de informação constantes da legislação comunitária, os Estados-Membros assegurarão que as comunicações

[38] JO L 145 de 13.6.1997, p. 1. Diretiva com a última redação que lhe foi dada pela Diretiva 1999/85/CE (JO L 277 de 28.10.1999, p. 34).

comerciais que constituam ou sejam parte de um serviço da sociedade da informação respeitem as condições seguintes:
a) A comunicação comercial deve ser claramente identificável como tal;

b) A pessoa singular ou coletiva por conta de quem a comunicação comercial é feita deve ser claramente identificável;

c) Quando autorizadas pelo Estado-Membro onde o prestador de serviços esteja estabelecido, as ofertas promocionais, tais como descontos, prémios e presentes, serão claramente identificáveis como tais e as condições a preencher para neles participar devem ser facilmente acessíveis e apresentadas de forma clara e inequívoca;

d) Quando autorizados pelo Estado-Membro onde o prestador de serviços esteja estabelecido, os concursos ou jogos promocionais devem ser claramente identificáveis como tal e as condições a preencher para neles participar devem ser facilmente acessíveis e apresentadas de forma clara e inequívoca.

Artigo 7.º Comunicação comercial não solicitada
1. Além de outros requisitos de informação constantes da legislação comunitária, os Estados-Membros que permitam a comunicação comercial não solicitada por correio eletrónico por parte de um prestador de serviços estabelecido no seu território assegurarão que essa comunicação comercial seja identificada como tal, de forma clara e inequívoca, a partir do momento em que é recebida pelo destinatário.

2. Sem prejuízo da Diretiva 97/7/CE e da Diretiva 97/66/CE, os Estados-Membros deverão tomar medidas que garantam que os prestadores de serviços que enviem comunicações comerciais não solicitadas por correio eletrónico consultem regularmente e respeitem os registos de opção negativa «opt-out») onde se podem inscrever as pessoas singulares que não desejem receber esse tipo de comunicações.

Artigo 8.º Profissões regulamentadas
1. Os Estados-Membros assegurarão que a utilização de comunicações comerciais que constituam ou sejam parte de um serviço da sociedade da informação prestado por um oficial de uma profissão regulamentada seja autorizada mediante sujeição ao cumprimento das regras profissionais

em matéria de independência, dignidade e honra da profissão, bem como do sigilo profissional e da lealdade para com clientes e outros membros da profissão.

2. Sem prejuízo da autonomia das organizações e associações profissionais, os Estados-Membros e a Comissão incentivarão as associações e organizações profissionais a elaborar códigos de conduta a nível comunitário, que permitam determinar os tipos de informações que podem ser prestadas para efeitos de comunicação comercial de acordo com as regras a que se refere o n.º 1.

3. Ao redigir propostas de iniciativas comunitárias que se revelem eventualmente necessárias para garantir o correto funcionamento do mercado interno no que respeita às informações previstas no n.º 2, a Comissão terá em devida conta os códigos de conduta aplicáveis a nível comunitário e agirá em estreita cooperação com as associações e organizações profissionais relevantes.

4. A presente diretiva é aplicável complementarmente às diretivas comunitárias relativas ao acesso às profissões regulamentadas e ao seu exercício.

SECÇÃO 3
CONTRATOS CELEBRADOS POR MEIOS ELETRÓNICOS

Artigo 9.º Regime dos contratos

1. Os Estados-Membros assegurarão que os seus sistemas legais permitam a celebração de contratos por meios eletrónicos. Os Estados-Membros assegurarão, nomeadamente, que o regime jurídico aplicável ao processo contratual não crie obstáculos à utilização de contratos celebrados por meios eletrónicos, nem tenha por resultado a privação de efeitos legais ou de validade desses contratos, pelo facto de serem celebrados por meios eletrónicos.

2. Os Estados-Membros podem determinar que o n.º 1 não se aplica a todos ou a alguns contratos que se inserem numa das categorias seguintes:
a) Contratos que criem ou transfiram direitos sobre bens imóveis, com exceção de direitos de arrendamento;

b) Contratos que exijam por lei a intervenção de tribunais, entidades públicas ou profissões que exercem poderes públicos;

c) Contratos de caução e garantias prestadas por pessoas agindo para fins exteriores à sua atividade comercial, empresarial ou profissional;

d) Contratos regidos pelo direito de família ou pelo direito sucessório.

3. Os Estados-Membros indicarão à Comissão as categorias a que se refere o n.º 2 às quais não aplicam o disposto no n.º 1. De cinco em cinco anos, os Estados-Membros apresentarão à Comissão um relatório sobre a aplicação do n.º 2, em que exporão as razões pelas quais consideram necessário manter à categoria contemplada na alínea b) do n.º 2 a que não aplicam o disposto no n.º 1.

Artigo 10.º Informações a prestar
1. Além de outros requisitos de informação constantes da legislação comunitária, os Estados-Membros assegurarão, salvo acordo em contrário das partes que não sejam consumidores, e antes de ser dada a ordem de encomenda pelo destinatário do serviço, que, no mínimo, o prestador de serviços preste em termos exatos, compreensíveis e inequívocos, a seguinte informação:
a) As diferentes etapas técnicas da celebração do contrato;

b) Se o contrato celebrado será ou não arquivado pelo prestador do serviço e se será acessível;

c) Os meios técnicos que permitem identificar e corrigir os erros de introdução anteriores à ordem de encomenda;

d) As línguas em que o contrato pode ser celebrado.

2. Os Estados-Membros assegurarão, salvo acordo em contrário das partes que não sejam consumidores, que o prestador indique os eventuais códigos de conduta de que é subscritor e a forma de consultar eletronicamente esses códigos.

3. Os termos contratuais e as condições gerais fornecidos ao destinatário têm de sê-lo numa forma que lhe permita armazená-los e reproduzi-los.

4. Os n.os 1 e 2 não são aplicáveis aos contratos celebrados exclusivamente por correio eletrónico ou outro meio de comunicação individual equivalente.

Artigo 11.º Ordem de encomenda
1. Os Estados-Membros assegurarão, salvo acordo em contrário das partes que não sejam consumidores, que, nos casos em que o destinatário de um serviço efetue a sua encomenda exclusivamente por meios eletrónicos, se apliquem os seguintes princípios:
- o prestador de serviços tem de acusar a receção da encomenda do destinatário do serviço, sem atraso injustificado e por meios eletrónicos,
- considera-se que a encomenda e o aviso de receção são recebidos quando as partes a que são endereçados têm possibilidade de aceder a estes.

2. Os Estados-Membros assegurarão, salvo acordo em contrário das partes que não sejam consumidores, que o prestador de serviços ponha à disposição do destinatário do serviço os meios técnicos adequados, eficazes e acessíveis, que lhe permitam identificar e corrigir erros de introdução antes de formular a ordem de encomenda.

3. O n.º 1, primeiro travessão, e o n.º 2 não são aplicáveis aos contratos celebrados exclusivamente por correio eletrónico ou outro meio de comunicação individual equivalente.

SECÇÃO 4
RESPONSABILIDADE DOS PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS

Artigo 12.º Simples transporte
1. No caso de prestações de um serviço da sociedade da informação que consista na transmissão, através de uma rede de comunicações, de informações prestadas pelo destinatário do serviço ou em facultar o acesso a uma rede de comunicações, os Estados-Membros velarão por que a responsabilidade do prestador não possa ser invocada no que respeita às informações transmitidas, desde que o prestador:
a) Não esteja na origem da transmissão;

b) Não selecione o destinatário da transmissão; e

c) Não selecione nem modifique as informações que são objeto da transmissão.

2. As atividades de transmissão e de facultamento de acesso mencionadas no n.º 1 abrangem a armazenagem automática, intermédia e transitória das informações transmitidas, desde que essa armazenagem sirva exclusivamente para a execução da transmissão na rede de comunicações e a sua duração não exceda o tempo considerado razoavelmente necessário a essa transmissão.

3. O disposto no presente artigo não afeta a possibilidade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infração.

Artigo 13.º Armazenagem temporária («caching»)
1. Em caso de prestação de um serviço da sociedade da informação que consista na transmissão, por uma rede de telecomunicações, de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à armazenagem automática, intermédia e temporária dessa informação, efetuada apenas com o objetivo de tornar mais eficaz a transmissão posterior da informação a pedido de outros destinatários do serviço, desde que:
a) O prestador não modifique a informação;

b) O prestador respeite as condições de acesso à informação;

c) O prestador respeite as regras relativas à atualização da informação, indicadas de forma amplamente reconhecida e utilizada pelo sector;

d) O prestador não interfira com a utilização legítima da tecnologia, tal como amplamente reconhecida e seguida pelo sector, aproveitando-a para obter dados sobre a utilização da informação; e

e) O prestador atue com diligência para remover ou impossibilitar o acesso à informação que armazenou, logo que tome conhecimento efetivo de que a informação foi removida da rede na fonte de transmissão inicial, de que o acesso a esta foi tornado impossível, ou de que um tribunal ou

autoridade administrativa ordenou essa remoção ou impossibilitação de acesso.

2. O disposto no presente artigo não afeta a possibilidade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infração.

Artigo 14.º Armazenagem em servidor
1. Em caso de prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à informação armazenada a pedido de um destinatário do serviço, desde que:
a) O prestador não tenha conhecimento efetivo da atividade ou informação ilegal e, no que se refere a uma ação de indemnização por perdas e danos, não tenha conhecimento de factos ou de circunstâncias que evidenciam a atividade ou informação ilegal, ou

b) O prestador, a partir do momento em que tenha conhecimento da ilicitude, atue com diligência no sentido de retirar ou impossibilitar o acesso às informações.

2. O n.º 1 não é aplicável nos casos em que o destinatário do serviço atue sob autoridade ou controlo do prestador.

3. O disposto no presente artigo não afeta a faculdade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infração, nem afeta a faculdade de os Estados-Membros estabelecerem disposições para a remoção ou impossibilitação do acesso à informação.

Artigo 15.º Ausência de obrigação geral de vigilância
1. Os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços mencionados nos artigos 12.º, 13.º e 14.º, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem ilicitudes.

2. Os Estados-Membros podem estabelecer a obrigação, relativamente aos prestadores de serviços da sociedade da informação, de que informem prontamente as autoridades públicas competentes sobre as atividades empreendidas ou informações ilícitas prestadas pelos autores aos destinatários dos serviços por eles prestados, bem como a obrigação de comunicar às autoridades competentes, a pedido destas, informações que permitam a identificação dos destinatários dos serviços com quem possuam acordos de armazenagem.

CAPÍTULO III
APLICAÇÃO

Artigo 16.º Código de conduta

1. Os Estados-Membros e a Comissão incentivarão:

a) A redação, pelas associações e organizações de comerciantes, profissionais ou de consumidores, de códigos de conduta a nível comunitário, destinados a contribuir para a correta aplicação dos artigos 5.º a 15.º;

b) A transmissão voluntária dos projetos de códigos de conduta, a nível nacional ou comunitário, à Comissão;

c) A acessibilidade, por via eletrónica, dos códigos de conduta nas línguas comunitárias;

d) A comunicação aos Estados-Membros e à Comissão, pelas associações e organizações de comerciantes, de profissionais ou de consumidores, das avaliações da aplicação dos seus códigos de conduta e o impacto desses códigos nas práticas, usos ou costumes relativos ao comércio eletrónico;

e) A redação de códigos de conduta em matéria de proteção dos menores e da dignidade humana.

2. Os Estados-Membros e a Comissão incentivarão a participação das associações e organizações representativas dos consumidores no processo de elaboração e aplicação dos códigos de conduta que dizem respeito aos seus interesses e sejam elaborados de acordo com a alínea a) do n.º 1. Sempre que adequado, as associações representativas dos deficientes visuais e outros deverão ser consultadas para ter em conta as necessidades específicas destes.

Artigo 17.º Resolução extrajudicial de litígios
1. Os Estados-Membros devem assegurar que, em caso de desacordo entre o prestador de um serviço da sociedade da informação e o destinatário desse serviço, a sua legislação não impeça a utilização de mecanismos de resolução extrajudicial disponíveis nos termos da legislação nacional para a resolução de litígios, inclusive através de meios eletrónicos adequados.

2. Os Estados-Membros incentivarão os organismos responsáveis pela resolução extrajudicial, designadamente dos litígios de consumidores, a que funcionem de forma a proporcionar adequadas garantias de procedimento às partes interessadas.

3. Os Estados-Membros incentivarão os organismos responsáveis pela resolução extrajudicial de litígios a informar a Comissão das decisões significativas tomadas relativamente aos serviços da sociedade da informação, bem como das práticas, usos ou costumes relativos ao comércio eletrónico.

Artigo 18.º Ações judiciais
1. Os Estados-Membros assegurarão que as ações judiciais disponíveis em direito nacional em relação às atividades de serviços da sociedade da informação permitam a rápida adoção de medidas, inclusive medidas transitórias, destinadas a pôr termo a alegadas infrações e a evitar outros prejuízos às partes interessadas.

2. *(Revogado)*

Artigo 19.º Cooperação
1. Os Estados-Membros disporão dos meios apropriados de controlo e de investigação necessários à aplicação eficaz da presente diretiva e assegurarão que os prestadores de serviços lhes comuniquem as informações requeridas.

2. Os Estados-Membros cooperarão com os outros Estados-Membros; para o efeito, designarão um ou mais pontos de contacto, cujos elementos de contacto comunicarão aos demais Estados-Membros e à Comissão.

3. Os Estados-Membros prestarão, com a maior celeridade e de acordo com a sua legislação nacional, a assistência e as informações solicitadas

por outros Estados-Membros ou pela Comissão, inclusive pelos meios eletrónicos adequados.

4. Os Estados-Membros estabelecerão pontos de contacto acessíveis pelo menos por via electrónica, aos quais os destinatários e os prestadores de serviços se podem dirigir para:
a) Obter informações de carácter geral sobre direitos e obrigações em matéria contratual, bem como sobre os mecanismos de reclamação e correção disponíveis em caso de litígio, inclusive sobre os aspetos práticos da utilização desses mecanismos;

b) Obter os elementos de contacto das autoridades, associações ou organizações junto das quais podem obter mais informações ou assistência prática.

5. Os Estados-Membros incentivarão a comunicação à Comissão das decisões administrativas e judiciais significativas tomadas no seu território sobre litígios relativos aos serviços da sociedade da informação, bem como sobre práticas, usos ou costumes relativos ao comércio eletrónico. A Comissão comunicará essas decisões aos outros Estados-Membros.

Artigo 20.º Sanções
Os Estados-Membros determinarão o regime das sanções aplicáveis às infrações às disposições nacionais adotadas em aplicação da presente diretiva e tomarão todas as medidas necessárias para garantir a respetiva aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

CAPÍTULO IV
DISPOSIÇÕES FINAIS

Artigo 21.º Relatório
1. Antes de 17 de Julho de 2003 e, seguidamente, de dois em dois anos, a Comissão apresentará ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social um relatório sobre a aplicação da presente diretiva, acompanhado, se for caso disso, de propostas de adaptação à evolução legislativa, técnica e económica dos serviços da sociedade da informação, em especial em matéria de prevenção do crime, de proteção de menores e dos consumidores e ao adequado funcionamento do mercado interno.

2. O referido relatório, ao examinar a necessidade de adaptação da presente diretiva, analisará, em particular, a necessidade de propostas relativas à responsabilidade dos prestadores de hiperligações e de instrumentos de localização, aos procedimentos de «*notice and take down*» e à atribuição de responsabilidade após a retirada do conteúdo. O relatório analisará igualmente a necessidade de prever condições suplementares para a isenção de responsabilidades a que se referem os artigos 12.º e 13.º, à luz da evolução da técnica, e a possibilidade de aplicar os princípios do mercado interno às comunicações comerciais não solicitadas por correio eletrónico.

Artigo 22.º Execução
1. Os Estados-Membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva, até 17 de Janeiro de 2002. Do facto informarão imediatamente a Comissão.

2. Sempre que os Estados-Membros aprovarem as disposições previstas no n.º 1, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência na publicação oficial. As modalidades dessa referência serão aprovadas pelos Estados-Membros.

Artigo 23.º Entrada em vigor
A presente diretiva entra em vigor na data da sua publicação no Jornal Oficial das Comunidades Europeias.

Artigo 24.º Destinatários
Os Estados-Membros são os destinatários da presente diretiva.

ANEXO
DERROGAÇÕES AO ARTIGO 3.º

Tal como refere o n.º 3 do artigo 3.º, os n.^{os} 1 e 2 desse artigo não são aplicáveis:
- aos direitos de autor, aos direitos conexos, aos direitos enunciados na Diretiva 87/54/CEE[39] e na Diretiva 96/9/CE[40], bem como aos direitos de propriedade industrial,

[39] *JO L 24 de 27.1.1987, p. 36.*
[40] *JO L 77 de 27.3.1996, p. 20.*

- à emissão de moeda eletrónica por instituições relativamente às quais os Estados-Membros tenham aplicado uma das derrogações previstas no n.º 1 do artigo 8.º da Diretiva 2000/46/CE[41],
- ao n.º 2 do artigo 44.º da Diretiva 85/611/CEE[42],
- ao artigo 30.º e ao título IV da Diretiva 92/49/CEE[43], ao título IV da Diretiva 92/96/CEE[44], aos artigos 7.º e 8.º da Diretiva 88/357/CEE[45] e ao artigo 4.º da Diretiva 90/619/CEE[46],
- à liberdade de as partes escolherem a legislação aplicável ao seu contrato,
- às obrigações contratuais relativas aos contratos celebrados pelos consumidores,
- à validade formal dos contratos que criem ou transfiram direitos sobre bens imóveis, sempre que esses contratos estejam sujeitos a requisitos de forma obrigatórios por força da lei do Estado-Membro onde se situa o bem imóvel,
- à autorização de comunicações comerciais não solicitadas por correio eletrónico.

Feito no Luxemburgo, em 8 de Junho de 2000.

Pelo Parlamento Europeu

A Presidente
N. FONTAINE

Pelo Conselho

O Presidente
G. d'OLIVEIRA MARTINS

---

[41] Ainda não publicada no Jornal Oficial.

[42] JO L 375 de 31.12.1985, p. 3. Diretiva com a última redação que lhe foi dada pela Diretiva 95/26/CE (JO L 168 de 18.7.1995, p. 7).

[43] JO L 228 de 11.8.1992, p. 1. Diretiva com a última redação que lhe foi dada pela Diretiva 95/26/CE.

[44] JO L 360 de 9.12.1992, p. 1. Diretiva com a última redação que lhe foi dada pela Diretiva 95/26/CE.

[45] JO L 172 de 4.7.1988, p. 1. Diretiva com a última redação que lhe foi dada pela Diretiva 92/49/CEE.

[46] JO L 330 de 29.11.1990, p. 50. Diretiva com a última redação que lhe foi dada pela Diretiva 92/96/CEE.

11. Lei nº 32/2008, de 17 de Julho transpõe para a ordem jurídica interna a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações - Lei da Retenção de Dados

Artigo 1.º Objeto

1. A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Junho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

2. A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações.

Artigo 2.º Definições

1. Para efeitos da presente lei, entende-se por:

a) «Dados», os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) «Serviço telefónico», qualquer dos seguintes serviços:

i) Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados;

ii) Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e

iii) Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS);

c) «Código de identificação do utilizador» («user ID»), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à Internet, ou num serviço de comunicação pela Internet;

d) «Identificador de célula» («cell ID»), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

e) «Chamada telefónica falhada», uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede;

f) «Autoridades competentes», as autoridades judiciárias e as autoridades de polícia criminal das seguintes entidades:
i) A Polícia Judiciária;

ii) A Guarda Nacional Republicana;

iii) A Polícia de Segurança Pública;

iv) A Polícia Judiciária Militar;

v) O Serviço de Estrangeiros e Fronteiras;

vi) A Polícia Marítima;

g) «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

2. Para efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes das Leis n.^{os}67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto.

Artigo 3.º Finalidade do tratamento
1. A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes.

2. A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º

3. Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins.

4. O titular dos dados não pode opor-se à respetiva conservação e transmissão.

Artigo 4.º Categorias de dados a conservar
1. Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:
a) Dados necessários para encontrar e identificar a fonte de uma comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;

d) Dados necessários para identificar o tipo de comunicação;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

2. Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:
a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:
i) O número de telefone de origem;

ii) O nome e endereço do assinante ou do utilizador registado;

b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:
i) Os códigos de identificação atribuídos ao utilizador;

ii) O código de identificação do utilizador e o número de telefone atribuídos

a qualquer comunicação que entre na rede telefónica pública;

iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.

3. Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:
a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:
i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;

ii) O nome e o endereço do assinante, ou do utilizador registado;

b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:
i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;

ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4. Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:
a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:
i) A data e a hora do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

ii) A data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5. Para os efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:
a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6. Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:
a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) No que diz respeito às comunicações telefónicas na rede móvel:
i) Os números de telefone de origem e de destino;

ii) A Identidade Internacional de Assinante Móvel (International Mobile Subscriber Identity, ou IMSI) de quem telefona;

iii) A Identidade Internacional do Equipamento Móvel (International Mobile Equipment Identity, ou IMEI) de quem telefona;

iv) A IMSI do destinatário do telefonema;

v) A IMEI do destinatário do telefonema;

vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado;

c) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:
i) O número de telefone que solicita o acesso por linha telefónica;

ii) A linha de assinante digital (digital subscriber line, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

7. Para os efeitos do disposto na alínea f) do n.º 1, os dados necessários

para identificar a localização do equipamento de comunicação móvel são os seguintes:
a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.

Artigo 5.º Âmbito da obrigação de conservação dos dados
1. Os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelas entidades referidas no n.º 1 do artigo 4.º, no contexto da oferta de serviços de comunicação.

2. Os dados relativos a chamadas não estabelecidas não são conservados.

Artigo 6.º Período de conservação
As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.

Artigo 7.º Proteção e segurança dos dados
1. As entidades referidas no n.º 1 do artigo 4.º devem:
a) Conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do juiz, às autoridades competentes;

b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos à mesma proteção e segurança que os dados na rede;

c) Tomar as medidas técnicas e organizativas adequadas à proteção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

d) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º;

e) Destruir os dados no final do período de conservação, exceto os dados que tenham sido preservados por ordem do juiz;

f) Destruir os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do juiz.

2. Os dados referentes às categorias previstas no artigo 4.º, com exceção dos dados relativos ao nome e endereço dos assinantes, devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes.

3. A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.

4. O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos nas Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto.

5. A autoridade pública competente para o controlo da aplicação do disposto no presente artigo é a Comissão Nacional de Proteção de Dados (CNPD).

Artigo 8.º Registo de pessoas especialmente autorizadas
1. A CNPD deve manter um registo eletrónico permanentemente atualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea d) do n.º 1 do artigo anterior.

2. Para os efeitos previstos no número anterior, os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações devem remeter à CNPD, por via exclusivamente eletrónica, os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados.

Artigo 9.º Transmissão dos dados
1. A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de

instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves.

2. A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3. Só pode ser autorizada a transmissão de dados relativos:
a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respetivo consentimento, efetivo ou presumido.

4. A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à proteção do segredo profissional, nos termos legalmente previstos.

5. O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6. As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extração dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.

Artigo 10.º Condições técnicas da transmissão dos dados
A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança previstas no n.º 3 do artigo 7.º

Artigo 11.º Destruição dos dados
1. O juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades

competentes, bem como dos dados preservados pelas entidades referidas no n.º 1 do artigo 4.º, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam.

2. Considera-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:
a) Arquivamento definitivo do processo penal;

b) Absolvição, transitada em julgado;

c) Condenação, transitada em julgado;

d) Prescrição do procedimento penal;

e) Amnistia.

Artigo 12.º Contraordenações
1. Sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, constitui contraordenação:
a) A não conservação das categorias dos dados previstas no artigo 4.º;

b) O incumprimento do prazo de conservação previsto no artigo 6.º;

c) A não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 9.º;

d) O não envio dos dados necessários à identificação das pessoas especialmente autorizadas, nos termos do n.º 2 do artigo 8.º

2. As contraordenações previstas no número anterior são puníveis com coimas de € 1500 a € 50 000 ou de € 5000 a € 10 000 000 consoante o agente seja uma pessoa singular ou coletiva.

3. A tentativa e a negligência são puníveis.

Artigo 13.º Crimes
1. Constituem crime, punido com pena de prisão até dois anos ou multa até 240 dias:
a) O incumprimento de qualquer das regras relativas à proteção e à segurança dos dados previstas no artigo 7.º;

b) O não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º;

c) O acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º

2. A pena é agravada para o dobro dos seus limites quando o crime:
a) For cometido através de violação de regras técnicas de segurança;

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais; ou

c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

3. A tentativa e a negligência são puníveis.

Artigo 14.º Processos de contraordenação e aplicação das coimas
1. Compete à CNPD a instrução dos processos de contraordenação e a respetiva aplicação de coimas relativas às condutas previstas no artigo anterior.

2. O montante das importâncias cobradas em resultado da aplicação das coimas é distribuído da seguinte forma:
a) 60 % para o Estado;

b) 40 % para a CNPD.

Artigo 15.º Aplicabilidade dos regimes sancionatórios previstos nas Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto
O disposto nos artigos 12.º a 14.º não prejudica a aplicação do disposto no capítulo vi da Lei n.º 67/98, de 26 de Outubro, e no capítulo iii da Lei n.º 41/2004, de 18 de Agosto.

Artigo 16.º Estatísticas para informação anual à Comissão das Comunidades Europeias
1. A CNPD transmite anualmente à Comissão das Comunidades Europeias as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações.

2. Tendo em vista o cumprimento do disposto no número anterior, as entidades referidas no n.º 1 do artigo 4.º devem, até 1 de Março de cada ano, remeter à CNPD as seguintes informações, relativas ao ano civil anterior:
a) O número de casos em que foram transmitidas informações às autoridades nacionais competentes;

b) O período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão; e

c) O número de casos em que as solicitações das autoridades não puderam ser satisfeitas.

3. As informações previstas no número anterior não podem conter quaisquer dados pessoais.

Artigo 17.º Avaliação
No fim de cada período de dois anos a CNPD, em colaboração com o Instituto das Comunicações de Portugal - Autoridade Nacional de Comunicações (ICP-ANACOM), procede a uma avaliação de todos os procedimentos previstos na presente lei e elabora um relatório detalhado, o qual pode incluir recomendações, cujo conteúdo deve ser transmitido à Assembleia da República e ao Governo.

Artigo 18.º Produção de efeitos
A presente lei produz efeitos 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º

Aprovada em 23 de Maio de 2008.
O Presidente da Assembleia da República, Jaime Gama.
Promulgada em 1 de Julho de 2008. Publique-se.
O Presidente da República, Aníbal Cavaco Silva.
Referendada em 2 de Julho de 2008.
O Primeiro-Ministro, José Sócrates Carvalho Pinto de Sousa.

12. Diretiva nº 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva n.º 2002/58/CE[47]

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia, nomeadamente o artigo 95º,

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Comité Económico e Social Europeu[48],

Deliberando nos termos do artigo 251.º do Tratado[49],

Considerando o seguinte:

1 // A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[50], exige aos Estados-Membros que protejam os direitos e as liberdades das pessoas singulares no que respeita ao tratamento de dados pessoais, nomeadamente o seu direito à privacidade, com o objetivo de assegurar a livre circulação de dados pessoais na Comunidade.

2 // A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade dos dados nas comunicações eletrónicas)[51], transpõe os

---

[47] Declarada inválida por força do Acórdão TJUE (Sala Grande Secção) 8 abril 2014.

[48] Parecer emitido em 19 de Janeiro de 2006 (ainda não publicado no Jornal Oficial).

[49] Parecer do Parlamento Europeu de 14 de Dezembro de 2005 (ainda não publicado no Jornal Oficial) e Decisão do Conselho de 21 de Fevereiro de 2006.

[50] JO L 281 de 23.11.1995, p. 31. Diretiva alterada pelo Regulamento (CE) n.º 1882/2003 (JO L 284 de 31.10.2003, p. 1).

[51] JO L 201 de 31.7.2002, p. 37.

princípios estabelecidos na Diretiva 95/46/CE para regras específicas do sector das comunicações eletrónicas.

3 // Os artigos 5.º, 6.º e 9.º da Diretiva 2002/58/CE definem as regras aplicáveis ao tratamento, pelos fornecedores de redes e de serviços, dos dados de tráfego e dos dados de localização gerados pela utilização de serviços de comunicações eletrónicas. Estes dados devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, exceto os dados necessários para efeitos de faturação e de pagamento de interligações. Mediante consentimento dos interessados, alguns dados podem igualmente ser tratados para efeitos de comercialização dos serviços de comunicações eletrónicas ou de fornecimento de serviços de valor acrescentado.

4 // O n.º 1 do artigo 15.o da Diretiva 2002/58/CE enumera as condições em que os Estados-Membros podem restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1, 2, 3 e 4 do artigo 8.º e no artigo 9.º da supracitada diretiva. Qualquer restrição deste tipo deve constituir uma medida necessária, adequada e proporcionada numa sociedade democrática, por razões específicas de ordem pública, ou seja, para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas.

5 // Vários Estados-Membros aprovaram legislação relativa à conservação de dados pelos fornecedores de serviços tendo em vista a prevenção, investigação, deteção e repressão de infrações penais. As disposições das diferentes legislações nacionais variam consideravelmente.

6 // As disparidades legislativas e técnicas existentes entre as disposições nacionais relativas à conservação dos dados para efeitos de prevenção, investigação, deteção e repressão de infrações penais constituem obstáculos ao mercado interno das comunicações eletrónicas; os fornecedores de serviços são obrigados a satisfazer exigências diferentes quanto aos tipos de dados de tráfego e de dados de localização a conservar, bem como às condições e aos períodos de conservação dos dados.

7 // Nas suas conclusões, o Conselho «Justiça e Assuntos Internos» de 19 de Dezembro de 2002 assinalou que, devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrónicas, os dados gerados pela utilização deste tipo de comunicações constituem um instrumento extremamente importante e útil na prevenção, investigação, deteção e de repressão de infrações penais, em especial contra a criminalidade organizada.

8 // Na sua Declaração de 25 de Março de 2004 sobre a luta contra o terrorismo, o Conselho Europeu encarregou o Conselho de proceder à análise de propostas relativas ao estabelecimento de regras sobre a conservação de dados de tráfego das comunicações pelos prestadores de serviços.

9 // Nos termos do artigo 8.o da Convenção Europeia dos Direitos do Homem (CEDH), qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência. As autoridades públicas só podem interferir no exercício deste direito nos termos previstos na lei e, quando essa ingerência for necessária, numa sociedade democrática, designadamente, para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infrações penais, ou a proteção dos direitos e das liberdades de terceiros. Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente diretiva. A aprovação de um instrumento de conservação de dados que obedeça aos requisitos do artigo 8.º da CEDH é, pois, uma medida necessária.

10 // Em 13 de Julho de 2005, na sua Declaração condenando os ataques terroristas em Londres, o Conselho reafirmou a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações.

11 // Tendo em consideração a importância dos dados de tráfego e dos dados de localização para a investigação, deteção e repressão de infrações penais, é necessário, como os trabalhos de investigação e a experiência

prática em vários Estados-Membros o demonstram, garantir a nível europeu a conservação durante um determinado período dos dados gerados ou tratados, no contexto da oferta de comunicações, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações, nas condições previstas na presente diretiva.

12 // O n.º 1 do artigo 15.º da Diretiva 2002/58/CE continua a ser aplicável aos dados, incluindo os relativos a chamadas telefónicas falhadas, cuja conservação não seja especificamente exigida pela presente diretiva e que, por conseguinte, não são abrangidos pelo seu âmbito de aplicação, bem como à conservação para efeitos não contemplados pela presente diretiva, incluindo fins judiciais.

13 // A presente diretiva diz unicamente respeito aos dados gerados ou tratados na sequência de uma comunicação ou de um serviço de comunicação e não se refere aos dados constituídos pelo conteúdo da informação comunicada. Os dados devem ser conservados de forma que evite a sua conservação repetida. Dados gerados ou tratados no momento da prestação dos serviços de comunicação em causa refere-se aos dados que são acessíveis. Em particular, quando se conservam dados relacionados com o correio eletrónico e a telefonia Internet, a obrigação de conservação pode ser imposta apenas em relação aos dados referentes aos serviços prestados pelos próprios fornecedores ou pelos fornecedores de serviços de rede.

14 // As tecnologias relacionadas com as comunicações eletrónicas evoluem rapidamente, e as exigências legítimas das autoridades competentes podem também evoluir. A fim de obter aconselhamento e de incentivar a partilha da experiência de boas práticas nesta matéria, a Comissão tenciona criar um grupo composto por autoridades responsáveis pela aplicação da lei nos Estados-Membros, associações do sector das comunicações eletrónicas, representantes do Parlamento Europeu e autoridades responsáveis pela proteção dos dados, nomeadamente a Autoridade Europeia para a Protecção de Dados.

15 // A Diretiva 95/46/CE e a Diretiva 2002/58/CE são plenamente aplicáveis aos dados conservados em conformidade com a presente diretiva. A alínea c) do n.º 1 do artigo 30.º da Diretiva 95/46/CE exige

a consulta do grupo de trabalho de proteção das pessoas no que respeita ao tratamento de dados pessoais, criado pelo artigo 29.º da dita diretiva.

16 // As obrigações que incumbem aos fornecedores de serviços, por força do artigo 6.º da Diretiva 95/46/CE, relativamente a medidas destinadas a assegurar a qualidade dos dados, e as obrigações dos mesmos de tomarem medidas para salvaguardar a confidencialidade e a segurança do tratamento de dados por força dos artigos 16.º e 17.º da referida diretiva, são plenamente aplicáveis aos dados conservados em conformidade com a presente diretiva.

17 // É essencial que os Estados-Membros tomem medidas legislativas para assegurar que os dados conservados por força da presente diretiva apenas sejam transmitidos às autoridades nacionais competentes em conformidade com a legislação nacional e no pleno respeito dos direitos fundamentais das pessoas em causa.

18 // Neste contexto, o artigo 24.º da Diretiva 95/46/CE obriga os Estados-Membros a determinar as sanções a aplicar em caso de violação das disposições adotadas nos termos dessa diretiva. O n.º 2 do artigo 15.º da Diretiva 2002/58/CE impõe a mesma obrigação relativamente às disposições nacionais aprovadas por força dessa diretiva. A Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação[52], dispõe que o acesso ilegal aos sistemas de informação, incluindo aos dados neles conservados, seja punível como infração penal.

19 // O direito, consagrado no artigo 23.º da Diretiva 95/46/CE, que assiste a qualquer pessoa que tenha sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato incompatível com as disposições nacionais de execução da mesma diretiva, de obter reparação pelo prejuízo sofrido, aplica-se igualmente ao tratamento ilícito de quaisquer dados pessoais, nos termos da presente diretiva.

20 // A Convenção do Conselho da Europa sobre a Cibercriminalidade, de 2001, e a Convenção do Conselho da Europa para a Protecção

[52] *JO L 69 de 16.3.2005, p. 67.*

das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, de 1981, também dizem respeito a dados conservados na aceção da presente diretiva.

21 // Atendendo a que os objetivos da presente diretiva, ou seja, a harmonização das obrigações que incumbem aos fornecedores de conservarem determinados dados e assegurarem que estes sejam disponibilizados para efeitos de investigação, deteção e repressão de crimes graves tal como definidos no direito nacional de cada Estado-Membro, não podem ser suficientemente realizados pelos Estados-Membros e podem, pois, devido à dimensão e aos efeitos da presente diretiva, ser melhor alcançados a nível comunitário, a Comunidade pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir aqueles objetivos.

22 // A presente diretiva respeita os direitos fundamentais e os princípios consagrados nomeadamente na Carta dos Direitos Fundamentais da União Europeia. Em especial, a presente diretiva, conjugada com a Diretiva 2002/58/CE, visa assegurar que sejam plenamente respeitados os direitos fundamentais dos cidadãos em matéria de respeito pela privacidade e pelas comunicações e de proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da Carta.

23 // Tendo em conta que as obrigações impostas aos fornecedores de serviços de comunicações eletrónicas devem ser proporcionadas, a presente diretiva estabelece que devem conservar apenas os dados gerados ou tratados no âmbito da prestação dos seus serviços de comunicações. Se esses dados não forem gerados ou tratados por esses fornecedores, estes não estão obrigados a conservá-los. A presente diretiva não visa a harmonização da tecnologia de conservação de dados, que deverá ser adotada a nível nacional.

24 // Em conformidade com o ponto 34 do Acordo Interinstitucional «Legislar Melhor»[53], os Estados-Membros são encorajados a elaborarem, para si próprios e no interesse da Comunidade, os seus próprios quadros, que ilustrem, na medida do possível, a concordância entre as diretivas e as medidas de transposição, e a publicá-los.

---

[53] *JO C 321 de 31.12.2003, p. 1.*

25 // A presente diretiva não prejudica o poder dos Estados-Membros de adotarem medidas legislativas respeitantes à utilização dos dados e ao direito de acesso aos mesmos por parte das autoridades nacionais por eles designados. As questões que se prendem com o acesso das autoridades nacionais aos dados conservados de acordo com a presente diretiva no contexto das atividades enumeradas no n.º 2 do artigo 3.o da Diretiva 95/46/CE não são abrangidas pelo direito comunitário. Todavia, podem estar sujeitas ao direito nacional ou a ações desenvolvidas ao abrigo do título VI do Tratado da União Europeia, no pressuposto de que estas leis ou ações respeitam plenamente os direitos fundamentais consagrados nas tradições constitucionais dos Estados-Membros e garantidos pela CEDH. O artigo 8.ºdesta Convenção, na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem, estabelece que a ingerência da autoridade pública no direito ao respeito da vida privada deve obedecer aos requisitos da necessidade e proporcionalidade, devendo servir para efeitos especificados, explícitos e legítimos e ser exercida de uma forma adequada, pertinente e não excessiva tendo em conta o objetivo pretendido,

ADOTARAM A PRESENTE DIRECTIVA:

Artigo 1.º Objeto e âmbito de aplicação

1. A presente diretiva visa harmonizar as disposições dos Estados--Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro.

2. A presente diretiva é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas, bem como aos dados conexos necessários para identificar o assinante ou o utilizador registado. A presente diretiva não é aplicável ao conteúdo das comunicações eletrónicas, incluindo as informações consultadas utilizando uma rede de comunicações eletrónicas.

Artigo 2.º Definições

1. Para efeitos da presente diretiva, são aplicáveis as definições constantes da Diretiva 95/46/CE, da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro)[54], e da Diretiva 2002/58/CE.

2. Para efeitos da presente diretiva, entende-se por:

a) «Dados», os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) «Utilizador», qualquer pessoa singular ou coletiva que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

c) «Serviço telefónico», os serviços de chamada (incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados), os serviços suplementares (incluindo o reencaminhamento e a transferência de chamadas) e os serviços de mensagens e multimédia [incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhorados (EMS) e os serviços multimédia (MMS)];

d) «Código de identificação de utilizador» («*user ID*»), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à internet, ou num serviço de comunicação pela internet;

e) «Identificador da célula» («*cell ID*»), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

f) «Chamada telefónica falhada», uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede.

Artigo 3.º Obrigação de conservação de dados

1. Em derrogação aos artigos 5.º, 6.º e 9.º da Diretiva 2002/58/CE, os Estados-Membros devem tomar medidas para garantir a conservação,

[54] *JO L 108 de 24.4.2002, p. 33.*

em conformidade com as disposições da presente diretiva, dos dados especificados no artigo 5.º da presente diretiva, na medida em que sejam gerados ou tratados no contexto da oferta dos serviços de comunicações em causa por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações quando estes fornecedores estejam sob a sua jurisdição.

2. A obrigação de conservação de dados imposta no n.º 1 inclui a conservação dos dados especificados no artigo 5.o relativos a chamadas telefónicas falhadas, quando gerados ou tratados, e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações, que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação. A presente diretiva não estabelece a conservação de dados relativos a chamadas não estabelecidas.

Artigo 4.º Acesso aos dados
Os Estados-Membros devem tomar medidas para assegurar que os dados conservados em conformidade com a presente diretiva só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. Os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado-Membro no respetivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem.

Artigo 5.º Categorias de dados a conservar
1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente diretiva:
a) Dados necessários para encontrar e identificar a fonte de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:
i) o número de telefone de origem,

ii) o nome e endereço do assinante ou do utilizador registado;

2) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
i) o(s) código(s) de identificação atribuído(s) ao utilizador,

ii) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública,

iii) o nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou o número de telefone estavam atribuídos no momento da comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:
i) o(s) número(s) marcados (o número ou números de telefone de destino) e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada,

ii) o nome e o endereço do assinante, ou do utilizador registado;

2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
i) o código de identificação de utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da internet,

ii) o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registado(s), e o código de identificação de utilizador do destinatário pretendido da comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

2) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
i) a data e a hora do início (*log-in*) e do fim (*log-off*) da ligação ao serviço de acesso à internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado,

ii) a data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da internet ou de comunicações telefónicas através da internet, com base em determinado fuso horário;

d) Dados necessários para identificar o tipo de comunicação:
1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel: o serviço telefónico utilizado;

2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet: o serviço internet utilizado;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:
1) no que diz respeito às comunicações telefónicas na rede fixa os números de telefone de origem e de destino;

2) no que diz respeito às comunicações telefónicas na rede móvel:
i) os números de telefone de origem e de destino,

ii) a Identidade Internacional de Assinante Móvel («*International Mobile Subscriber Identity*», ou IMSI) de quem telefona,

iii) a Identidade Internacional do Equipamento Móvel («*International Mobile Equipment Identity*», ou IMEI) de quem telefona,

iv) a IMSI do destinatário do telefonema,

v) a IMEI do destinatário do telefonema,

vi) no caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;

3) No que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:
i) o número de telefone que solicita o acesso por linha telefónica,

ii) a linha de assinante digital («*digital subscriber line*», ou DSL), ou qualquer outro identificador terminal do autor da comunicação;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel:
1) o identificador da célula no início da comunicação;

2) os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.

2. Nos termos da presente diretiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações.

Artigo 6.º Períodos de conservação
Os Estados-Membros devem assegurar que as categorias de dados referidos no artigo 5.º sejam conservadas por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação.

Artigo 7.º Proteção de dados e segurança dos dados
Sem prejuízo das disposições adotadas nos termos da Diretiva 95/46/CE e da Diretiva 2002/58/CE, cada Estado-Membro deve assegurar que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações respeitem, no mínimo, os seguintes princípios em matéria de segurança de dados no que se refere aos dados conservados em conformidade com a presente diretiva:
a) Os dados conservados devem ser da mesma qualidade e estar sujeitos à mesma proteção e segurança que os dados na rede;

b) Os dados devem ser objeto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental, ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

c) Os dados devem ser objeto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados; e

d) Os dados devem ser destruídos no final do período de conservação, exceto os dados que tenham sido facultados e preservados.

Artigo 8.º Requisitos para o armazenamento dos dados conservados
Os Estados-Membros devem assegurar que os dados especificados no artigo 5.º sejam conservados em conformidade com a presente diretiva de modo que tais dados e outras informações necessárias relacionadas com esses dados possam ser transmitidos imediatamente, mediante pedido, às autoridades competentes.

Artigo 9.º Autoridade de controlo
1. Cada Estado-Membro deve designar uma ou mais autoridades públicas para controlar a aplicação, no respetivo território, das disposições adotadas pelos Estados-Membros, nos termos do artigo 7.º, no que diz respeito à segurança dos dados conservados. Essas autoridades podem ser as referidas no artigo 28.º da Diretiva 95/46/CE.

2. As autoridades a que se refere o n.º 1 devem atuar com absoluta independência no exercício do controlo da aplicação a que se refere o mesmo número.

Artigo 10.º Estatísticas
1. Os Estados-Membros devem assegurar que sejam transmitidas anualmente à Comissão as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações. Estas estatísticas devem incluir:
— os casos em que foram transmitidas informações às autoridades competentes em conformidade com o direito nacional aplicável,
— o período de tempo decorrido entre a data a partir da qual os dados

foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão,
— os casos em que os pedidos de dados não puderam ser satisfeitos.

2. As referidas estatísticas não podem incluir dados pessoais.

Artigo 11.º Alteração da Diretiva 2002/58/CE
No artigo 15.º da Diretiva 2002/58/CE é inserido o seguinte número:
«1-A. O n.º 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (*), para os fins mencionados no n.º 1 do artigo 1.º dessa diretiva.

Artigo 12.º Medidas futuras
1. Um Estado-Membro que tenha de fazer face a circunstâncias especiais que justifiquem a prorrogação, por um prazo limitado, do período máximo de conservação previsto no artigo 6.º pode adotar as medidas necessárias. O Estado-Membro em questão deve notificar imediatamente a Comissão e informar os restantes Estados-Membros das medidas adotadas ao abrigo do presente artigo e deve indicar as razões que o levaram a adotá-las.

2. No prazo de seis meses após a notificação a que é feita referência no n.º 1, a Comissão deve aprovar ou rejeitar as medidas nacionais em questão depois de ter verificado se estas constituem ou não uma forma de discriminação arbitrária ou uma restrição dissimulada ao comércio entre os Estados-Membros ou se constituem ou não um obstáculo ao funcionamento do mercado interno. Se a Comissão não adotar qualquer decisão neste prazo, as medidas nacionais são consideradas aprovadas.

3. Nos casos em que, ao abrigo do n.º 2, forem aprovadas medidas nacionais adotadas por um Estado-Membro que derroguem as disposições da presente diretiva, a Comissão deve examinar se é necessário propor uma alteração da presente diretiva.

(*) JO L 105 de 13.4.2006, p. 54.».

Artigo 13.º Recursos, responsabilidade e sanções
1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as medidas nacionais que dão execução ao capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções sejam plenamente aplicadas no que se refere ao tratamento de dados no âmbito da presente diretiva.

2. Os Estados-Membros devem tomar, em particular, as medidas necessárias para assegurar que o acesso ou a transferência intencional de dados conservados em conformidade com a presente diretiva, não permitido pelo direito nacional adotado em virtude da presente diretiva, seja punível por sanções, incluindo sanções administrativas ou penais, que sejam efetivas, proporcionadas e dissuasivas.

Artigo 14.º Avaliação
1. A Comissão deve apresentar ao Parlamento Europeu e ao Conselho, até 15 de Setembro de 2010, uma avaliação sobre a aplicação da presente diretiva e os respetivos efeitos nos operadores económicos e nos consumidores, tendo em conta os progressos da tecnologia das comunicações eletrónicas e as estatísticas transmitidas à Comissão por força do artigo 10.o, a fim de determinar se é necessário alterar as disposições da presente diretiva, designadamente a lista dos dados referidos no artigo 5.º e os períodos de conservação previstos no artigo 6.o Os resultados da avaliação devem ser acessíveis ao público.

2. Para este efeito, a Comissão deve examinar todas as observações que lhe sejam transmitidas pelos Estados-Membros ou pelo grupo de trabalho instituído nos termos do artigo 29.o da Diretiva 95/46/CE.

Artigo 15.º Transposição
1. Os Estados-Membros devem pôr em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva o mais tardar em 15 de Setembro de 2007 e informar imediatamente a Comissão desse facto. Quando os Estados-Membros aprovarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da publicação oficial. As modalidades de referência são aprovadas pelos Estados-Membros.

2. Os Estados-Membros devem comunicar à Comissão o texto das principais disposições de direito interno que aprovarem nas matérias reguladas pela presente diretiva.

3. Até 15 de Março de 2009, cada Estado-Membro pode diferir a aplicação da presente diretiva no que se refere à conservação de dados relacionados com o acesso à internet, às comunicações telefónicas através da Internet e ao correio eletrónico através da internet. Os Estados-Membros que tencionem recorrer a este número devem, aquando da aprovação da presente diretiva, notificar desse facto o Conselho e a Comissão, por meio de uma declaração. A declaração será publicada no *Jornal Oficial da União Europeia*.

Artigo 16.º Entrada em vigor
A presente diretiva entra em vigor 20 dias após a sua publicação no *Jornal Oficial da União Europeia*.

Artigo 17.º Destinatários
Os Estados-Membros são os destinatários da presente diretiva.

Feito em Estrasburgo, em 15 de Março de 2006.

Pelo Parlamento Europeu

O Presidente
J. BORRELL FONTELLES

Pelo Conselho
O Presidente
H. WINKLER

13. Lei nº 41/2004 de 18 de Agosto, transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção de privacidade no sector das comunicações eletrónicas[55]

CAPÍTULO I
OBJETO E ÂMBITO

Artigo 1.º Objeto e âmbito de aplicação

1 // A presente lei transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, com as alterações determinadas pelo artigo 2.º da Diretiva n.º 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro.

2 // A presente lei aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação, especificando e complementando as disposições da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais).

3 // As disposições da presente lei asseguram a proteção dos interesses legítimos dos assinantes que sejam pessoas coletivas na medida em que tal proteção seja compatível com a sua natureza.

4 // As exceções à aplicação da presente lei que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais são definidas em legislação especial.

---

[55] Última modificação legislativa: Lei n.º 46/2012, de 29 de Agosto, transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

5 // Nas situações previstas no número anterior, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem estabelecer procedimentos internos que permitam responder aos pedidos de acesso a dados pessoais dos utilizadores apresentados pelas autoridades judiciárias competentes, em conformidade com a referida legislação especial.

Artigo 2.º Definições

1. Para efeitos da presente lei, entende-se por:

a) «Comunicação» qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público;

b) «Correio eletrónico» qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha;

c) «Utilizador» qualquer pessoa singular que utilize um serviço de comunicações eletrónicas acessível ao público para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

d) «Dados de tráfego» quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma;

e) «Dados de localização» quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

f) «Serviços de valor acrescentado» todos aqueles que requeiram o tratamento de dados de tráfego ou de dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma;

g) «Violação de dados pessoais» uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração,

a divulgação ou o acesso não autorizado a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público.

2. É excluída da alínea a) do número anterior toda a informação difundida ao público em geral, através de uma rede de comunicações eletrónicas, que não possa ser relacionada com o assinante de um serviço de comunicações eletrónicas ou com qualquer utilizador identificável que receba a informação.

3. Salvo definição específica da presente lei, são aplicáveis as definições constantes da Lei de Proteção de Dados Pessoais e da Lei n.º 5/2004, de 10 de fevereiro, na redação que lhe foi dada pela Lei n.º 51/2011, de 13 de setembro (Lei das Comunicações Eletrónicas).

CAPÍTULO II
SEGURANÇA E CONFIDENCIALIDADE

Artigo 3.º Segurança do processamento

1. As empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem adotar as medidas técnicas e organizacionais adequadas para garantir a segurança dos seus serviços, se necessário, no que respeita à segurança de rede, em conjunto com o fornecedor da rede pública de comunicações.

2. O fornecedor de rede pública de comunicações que sirva de suporte a serviços de comunicações eletrónicas acessíveis ao público, prestados por outra empresa deve satisfazer os pedidos que esta lhe apresente e que sejam necessários para o cumprimento do regime fixado na presente lei.

3. As medidas referidas no n.º 1 devem ser adequadas à prevenção dos riscos existentes, tendo em conta a proporcionalidade dos custos da sua aplicação e o estado da evolução tecnológica.

4. O ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) deve emitir recomendações sobre as melhores práticas relativas ao nível de segurança que essas medidas devem alcançar.

5. O ICP-ANACOM deve, diretamente ou através de entidade independente, auditar as medidas adotadas nos termos dos números anteriores.

6. O ICP-ANACOM deve estabelecer o plano dessas auditorias, de modo a abranger, nomeadamente, a determinação dos procedimentos e normas de referência a aplicar-lhes e os requisitos exigíveis aos auditores.

7. Pode ainda o ICP-ANACOM, ou uma entidade independente por si designada, realizar auditorias de segurança extraordinárias.

8. Para efeitos da aplicação dos n.os 4 a 7 do presente artigo, caso estejam em causa medidas que possam envolver matérias de proteção de dados pessoais, deve o ICP-ANACOM solicitar parecer à Comissão Nacional de Proteção de Dados (CNPD).

9. Sem prejuízo do disposto na Lei da Proteção de Dados Pessoais, as medidas referidas nos n.os 1 a 3 devem, no mínimo, incluir:
a) Medidas que assegurem que somente o pessoal autorizado possa ter acesso aos dados pessoais, e apenas para fins legalmente autorizados;

b) A proteção dos dados pessoais transmitidos, armazenados ou de outro modo tratados, contra a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados ou acidentais;

c) Medidas que assegurem a aplicação de uma política de segurança no tratamento dos dados pessoais.

10. Em caso de risco especial de violação da segurança da rede, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem informar gratuitamente os assinantes desses serviços da existência do risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis para evitá-lo e dos custos prováveis daí decorrentes.

Artigo 3.º-A Notificação de violação de dados pessoais
1. As empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem, sem demora injustificada, notificar a CNPD da ocorrência de violação de dados pessoais.

2. Quando a violação de dados pessoais referida no número anterior possa afetar negativamente os dados pessoais do assinante ou utilizador, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem ainda, sem demora injustificada, notificar a violação ao assinante ou ao utilizador, para que estes possam tomar as precauções necessárias.

3. Uma violação de dados pessoais afeta negativamente os dados ou a privacidade do assinante ou utilizador sempre que possa resultar, designadamente, em usurpação ou fraude de identidade, danos físicos, humilhação significativa ou danos para a reputação, quando associados à prestação e utilização de serviços de comunicações eletrónicas acessíveis ao público.

4. O regime previsto no n.º 2 não se aplica nos casos em que as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público comprovem perante a CNPD, e esta reconheça, que adotaram as medidas tecnológicas de proteção adequadas e que essas medidas foram aplicadas aos dados a que a violação diz respeito.

5. As medidas a que se refere o número anterior devem tornar os dados incompreensíveis para todas as pessoas não autorizadas a aceder-lhes.

6. Sem prejuízo da obrigação de notificação a que se refere o n.º 2, quando a empresa que oferece serviços de comunicações eletrónicas acessíveis ao público não tiver ainda notificado a violação de dados pessoais ao assinante ou ao utilizador, a CNPD pode exigir a realização da mesma notificação, tendo em conta a probabilidade de efeitos adversos decorrentes da violação.

7. Constituem elementos mínimos da notificação a que se refere o n.º 2 a identificação da natureza da violação dos dados pessoais e dos pontos de contato onde possam ser obtidas informações complementares, bem como a recomendação de medidas destinadas a limitar eventuais efeitos adversos da referida violação.

8. Na notificação à CNPD prevista no n.º 1, a empresa que oferece serviços de comunicações eletrónicas acessíveis ao público deve, além

dos elementos constantes do número anterior, indicar as consequências da violação de dados pessoais e as medidas por si propostas ou tomadas para fazer face à violação.

9. A CNPD pode, em conformidade com as decisões da Comissão Europeia, emitir orientações ou instruções sobre as circunstâncias em que as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público estão obrigadas a notificar a violação de dados pessoais, bem como sobre a forma e o procedimento aplicáveis a essas notificações.

10. Para a verificação, pela CNPD, do cumprimento das obrigações estabelecidas no presente artigo, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem constituir e manter um registo das situações de violação de dados pessoais, com indicação dos factos que lhes dizem respeito, dos seus efeitos e das medidas adotadas, incluindo as notificações efetuadas e as medidas de reparação tomadas.

Artigo 4.º Inviolabilidade das comunicações eletrónicas

1. As empresas que oferecem redes e ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público.

2. É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei.

3. O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transação comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.

4. São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

Artigo 5.º Armazenamento e acesso à informação
1. O armazenamento de informações e a possibilidade de acesso à informação armazenada no equipamento terminal de um assinante ou utilizador apenas são permitidos se estes tiverem dado o seu consentimento prévio, com base em informações claras e completas nos termos da Lei de Proteção de Dados Pessoais, nomeadamente quanto aos objetivos do processamento.

2. O disposto no presente artigo e no artigo anterior não impede o armaze-namento técnico ou o acesso:
a) Que tenha como única finalidade transmitir uma comunicação através de uma rede de comunicações eletrónicas;

b) Estritamente necessário ao fornecedor para fornecer um serviço da sociedade de informação solicitado expressamente pelo assinante ou utilizador.

Artigo 6.º Dados de tráfego
1. Sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações electrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2. É permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações, designadamente:
a) Número ou identificação, endereço e tipo de posto do assinante;

b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efetuadas ou o volume de dados transmitidos;

c) Data da chamada ou serviço e número chamado;

d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.

3. O tratamento referido no número anterior apenas é lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.

4. As empresas que oferecem serviços de comunicações eletrónicas só podem tratar os dados referidos no n.º 1 se o assinante ou utilizador a quem os dados digam respeito tiver dado o seu consentimento prévio e expresso, que pode ser retirado a qualquer momento, e apenas na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrónicas ou à prestação de serviços de valor acrescentado.

5. Nos casos previstos no n.º 2 e, antes de ser obtido o consentimento dos assinantes ou utilizadores, nos casos previstos no n.º 4, as empresas que oferecem serviços de comunicações eletrónicas devem fornecer-lhes informações exatas e completas sobre o tipo de dados que são tratados, os fins e a duração desse tratamento, bem como sobre a sua eventual disponibilização a terceiros para efeitos da prestação de serviços de valor acrescentado.

6. O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público encarregados da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas acessíveis ao público, ou da prestação de serviços de valor acrescentado, restringindo-se ao necessário para efeitos das referidas atividades.

7. O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação.

Artigo 7.º Dados de localização

1. Nos casos em que sejam processados dados de localização, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações eletrónicas acessíveis ao público, o tratamento destes dados é permitido apenas se os mesmos forem tornados anónimos.

2. É permitido o registo, tratamento e transmissão de dados de localização às organizações com competência legal para receber chamadas de emergência para efeitos de resposta a essas chamadas.

3. Do mesmo modo, o tratamento de dados de localização é permitido na medida e pelo tempo necessários para a prestação de serviços de valor acrescentado, desde que seja obtido consentimento prévio e expresso dos assinantes ou utilizadores.

4. As empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem, designadamente, informar os utilizadores ou assinantes, antes de obterem o seu consentimento, sobre o tipo de dados de localização que serão tratados, a duração e os fins do tratamento e a eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado.

5. As empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem garantir aos assinantes e utilizadores a possibilidade de, através de um meio simples e gratuito:

a) Retirar a qualquer momento o consentimento anteriormente concedido para o tratamento dos dados de localização referidos nos números anteriores;

b) Recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação.

6. O tratamento dos dados de localização deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público ou de terceiros que forneçam o serviço de valor acrescentado, devendo restringir-se ao necessário para efeitos da referida atividade.

Artigo 8.º Faturação detalhada
1. Os assinantes têm o direito de receber faturas não detalhadas.

2. As empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público devem conciliar os direitos dos assinantes que recebem faturas detalhadas com o direito à privacidade dos utilizadores autores das chamadas e dos assinantes chamados, nomeadamente submetendo à aprovação da CNPD propostas quanto a meios que permitam aos assinantes um acesso anónimo ou estritamente privado a serviços de comunicações eletrónicas acessíveis ao público.

3. A aprovação pela CNPD, referida no número anterior, está sujeita a parecer prévio obrigatório do ICP-ANACOM.
4. As chamadas facultadas ao assinante a título gratuito, incluindo chamadas para serviços de emergência ou de assistência, não devem constar da faturação detalhada.

Artigo 9.º Identificação da linha chamadora e da linha conectada
1. Quando for oferecida a apresentação da identificação da linha chamadora, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem garantir, linha a linha, aos assinantes que efetuam as chamadas e, em cada chamada, aos demais utilizadores a possibilidade de, através de um meio simples e gratuito, impedir a apresentação da identificação da linha chamadora.

2. Quando for oferecida a apresentação da identificação da linha chamadora, as empresas que oferecem serviços de comunicações eletrónicas devem garantir ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito, no caso de uma utilização razoável desta função, a apresentação da identificação da linha chamadora nas chamadas de entrada.

3. Nos casos em que seja oferecida a identificação da linha chamadora antes de a chamada ser atendida, as empresas que oferecem serviços de comunicações eletrónicas devem garantir ao assinante chamado a possibilidade de rejeitar, através de um meio simples, chamadas de entrada não identificadas.

4. Quando for oferecida a apresentação da identificação da linha conectada, as empresas que oferecem serviços de comunicações eletrónicas devem garantir ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito, a apresentação da identificação da linha conectada ao utilizador que efetua a chamada.

5. O disposto no n.º 1 do presente artigo é igualmente aplicável às chamadas para países que não pertençam à União Europeia originadas em território nacional.

6. O disposto nos n.os 2, 3 e 4 é igualmente aplicável a chamadas de entrada originadas em países que não pertençam à União Europeia.

7. As empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público são obrigadas a disponibilizar ao público, e em especial aos assinantes, informações transparentes e atualizadas sobre as possibilidades referidas nos números anteriores.

Artigo 10.º Exceções

1. As empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público devem, quando tal for compatível com os princípios da necessidade, da adequação e da proporcionalidade, anular por um período de tempo não superior a 30 dias a eliminação da apresentação da linha chamadora, a pedido, feito por escrito e devidamente fundamentado, de um assinante que pretenda determinar a origem de chamadas não identificadas perturbadoras da paz familiar ou da intimidade da vida privada, caso em que o número de telefone dos assinantes chamadores que tenham eliminado a identificação da linha é registado e comunicado ao assinante chamado.

2. Nos casos previstos no número anterior, a anulação da eliminação da apresentação da linha chamadora deve ser precedida de parecer obrigatório por parte da Comissão Nacional de Proteção de Dados.

3. As empresas referidas no n.º 1 devem igualmente anular, numa base linha a linha, a eliminação da apresentação da linha chamadora bem como registar e disponibilizar os dados de localização de um

assinante ou utilizador, no caso previsto no n.º 2 do artigo 7.º, por forma a disponibilizar esses dados às organizações com competência legal para receber chamadas de emergência para efeitos de resposta a essas chamadas.

4. Nos casos dos números anteriores, deve ser obrigatoriamente transmitida informação prévia ao titular dos referidos dados, sobre a transmissão dos mesmos, ao assinante que os requereu nos termos do n.º 1 ou aos serviços de emergência nos termos do n.º 3.

5. O dever de informação aos titulares dos dados deve ser exercido pelos seguintes meios:
a) Nos casos do n.º 1, mediante a emissão de uma gravação automática antes do estabelecimento da chamada, que informe os titulares dos dados que, a partir daquele momento e pelo prazo previsto, o seu número de telefone deixa de ser confidencial nas chamadas efetuadas para o assinante que pediu a identificação do número;
b) Nos casos do n.º 3, mediante a inserção de cláusulas contratuais gerais nos contratos a celebrar entre os assinantes e as empresas que fornecem redes e ou serviços de comunicações eletrónicas, ou mediante comunicação expressa aos assinantes nos contratos já celebrados, que possibilitem a transmissão daquelas informações aos serviços de emergência.

6. A existência do registo e da comunicação a que se referem os n.os 1 e 3 devem ser objeto de informação ao público e a sua utilização deve ser restringida ao fim para que foi concedida.

Artigo 11.º Reencaminhamento automático de chamadas
As empresas que oferecem redes e ou serviços de comunicações eletrónicas acessíveis ao público devem assegurar aos assinantes a possibilidade de, através de um meio simples e gratuito, interromper o reencaminhamento automático de chamadas efetuado por terceiros para o seu equipamento terminal.

Artigo 12.º Centrais digitais e analógicas
(Revogado)

Artigo 13.º Listas de assinantes

1. Os assinantes devem ser informados, gratuitamente e antes da inclusão dos respetivos dados em listas, impressas ou eletrónicas, acessíveis ao público ou que possam ser obtidas através de serviços de informação de listas, sobre:

a) Os fins a que as listas se destinam;

b) Quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões eletrónicas das listas.

2. Os assinantes têm o direito de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, decidir quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, tal como estipulado pelo fornecedor.

3. Deve ser garantida aos assinantes a possibilidade de, sem custos adicionais, verificar, corrigir, alterar ou retirar os dados incluídos nas referidas listas.

4. Deve ser obtido o consentimento adicional expresso dos assinantes para qualquer utilização de uma lista pública que não consista na busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação.

Artigo 13.º-A Comunicações não solicitadas

1. Está sujeito a consentimento prévio expresso do assinante que seja pessoa singular, ou do utilizador, o envio de comunicações não solicitadas para fins de marketing direto, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares.

2. O disposto no número anterior não se aplica aos assinantes que sejam pessoas coletivas, sendo permitidas as comunicações não solicitadas para fins de marketing direto até que os assinantes recusem futuras comunicações e se inscrevam na lista prevista no n.º 2 do artigo 13.º-B.

3. O disposto nos números anteriores não impede que o fornecedor de determinado produto ou serviço que tenha obtido dos seus clientes, nos termos da Lei de Proteção de Dados Pessoais, no contexto da venda de um produto ou serviço, as respetivas coordenadas eletrónicas de contacto, possa utilizá-las para fins de marketing direto dos seus próprios produtos ou serviços análogos aos transacionados, desde que garanta aos clientes em causa, clara e explicitamente, a possibilidade de recusarem, de forma gratuita e fácil, a utilização de tais coordenadas:
a) No momento da respetiva recolha; e

b) Por ocasião de cada mensagem, quando o cliente não tenha recusado inicialmente essa utilização.

4. É proibido o envio de correio eletrónico para fins de marketing direto, ocultando ou dissimulando a identidade da pessoa em nome de quem é efetuada a comunicação, em violação do artigo 21.º do Decreto-Lei n.º 7/2004, de 7 de janeiro, sem a indicação de um meio de contacto válido para o qual o destinatário possa enviar um pedido para pôr termo a essas comunicações, ou que incentive os destinatários a visitar sítios na Internet que violem o disposto no referido artigo.

5. Para tutela dos interesses dos seus clientes, como parte dos respetivos interesses comerciais, os prestadores de serviços de comunicações eletrónicas acessíveis ao público têm legitimidade para propor ações judiciais contra o autor do incumprimento de qualquer das disposições constantes do presente artigo, bem como do artigo 13.º-B.

Artigo 13.º-B Listas para efeitos de comunicações não solicitadas
1. Às entidades que promovam o envio de comunicações para fins de marketing direto, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares, cabe manter, por si ou por organismos que as representem, uma lista atualizada de pessoas que manifestaram expressamente e de forma gratuita o consentimento para a receção deste tipo de

comunicações, bem como dos clientes que não se opuseram à sua receção ao abrigo do n.º 3 do artigo 13.º-A.

2. Compete à Direção-Geral do Consumidor (DGC) manter atualizada uma lista de âmbito nacional de pessoas coletivas que manifestem expressamente opor-se à receção de comunicações não solicitadas para fins de marketing direto.

3. Pela inclusão nas listas referidas nos números anteriores não pode ser cobrada qualquer quantia.

4. A inserção na lista referida no n.º 2 depende do preenchimento de formulário eletrónico disponibilizado através da página eletrónica da DGC.

5. As entidades que promovam o envio de comunicações para fins de marketing direto são obrigadas a consultar a lista, atualizada mensalmente pela DGC, que a disponibiliza a seu pedido.

Artigo 13.º-C Cooperação transfronteiriça
1. Sem prejuízo das competências atribuídas a outras entidades, a CNPD e o ICP-ANACOM podem, nas respetivas áreas de competência, aprovar medidas para assegurar uma cooperação transfronteiriça eficaz na execução da presente lei.

2. Sempre que pretendam proceder nos termos previstos no número anterior, a CNPD e o ICP-ANACOM apresentam à Comissão Europeia, em tempo útil e antes da aprovação das medidas em causa, um resumo dos motivos para a ação, os requisitos previstos e as ações propostas.

Artigo 13.º-D Competências da CNPD e do ICP-ANACOM
No âmbito das competências que lhes são atribuídas pela presente lei, a CNPD e o ICP-ANACOM podem, nas respetivas áreas de competência:
a) Elaborar regulamentos relativamente às práticas a adotar para cumprimento da presente lei;

b) Dar ordens e formular recomendações;

c) Publicitar, nos respetivos sítios na Internet, os códigos de conduta de que tenha conhecimento;

d) Publicitar, nos respetivos sítios na Internet, outras informações que considerem relevantes.

Artigo 13.º-E Prestação de informações

1. As entidades sujeitas a obrigações nos termos da presente lei devem, quando solicitadas, prestar ao ICP-ANACOM, na sua respetiva área de competência, todas as informações relacionadas com a sua atividade, para que estas autoridades possam exercer todas as competências naquela previstas.

2. Os pedidos de informação a que se refere o número anterior devem obedecer a princípios de adequação ao fim a que se destinam e de proporcionalidade e devem ser devidamente fundamentados.

3. As informações solicitadas devem ser prestadas dentro dos prazos, na forma e com o grau de pormenor exigidos pelo ICP-ANACOM, que pode também estabelecer as circunstâncias e a periodicidade do seu envio.

4. Para efeitos do n.º 1, as entidades devem identificar, de forma fundamentada, as informações que consideram confidenciais e devem juntar, caso se justifique, uma cópia não confidencial dos documentos em que se contenham tais informações.

Artigo 13.º-F Incumprimento

1. Sem prejuízo de outros mecanismos sancionatórios aplicáveis, sempre que a CNPD ou o ICP-ANACOM, nas respetivas áreas de competência, verificarem a infração de qualquer obrigação decorrente da presente lei, devem notificar o infrator desse facto e dar-lhe a possibilidade de num prazo não inferior a 10 dias se pronunciar e, se for caso disso, pôr fim ao incumprimento.

2. Após ter procedido à audiência, nos termos do número anterior, a CNPD ou o ICP-ANACOM, nas respetivas áreas de competência, podem exigir ao infrator que cesse o incumprimento imediatamente ou no prazo razoável fixado para o efeito.

3. Se o infrator não puser fim ao incumprimento no prazo referido nos números anteriores, compete à CNPD ou ao ICP-ANACOM, nas respetivas

áreas de competência, tomar as medidas adequadas e proporcionais para garantir a observância das obrigações referidas no n.º 1 do presente artigo, nomeadamente a aplicação de sanções pecuniárias compulsórias nos termos previstos na presente lei.

Artigo 13.º-G Fiscalização
Compete à CNPD e ao ICP-ANACOM, nas respetivas áreas de competência estabelecidas nos termos do disposto no artigo 15.º, a fiscalização do cumprimento da presente lei, através, respetivamente, dos vogais e técnicos devidamente mandatados pela CNPD, nos termos da Lei de Proteção de Dados Pessoais e dos agentes de fiscalização ou de mandatários devidamente credenciados pelo ICP-ANACOM, nos termos do artigo 112.º da Lei das Comunicações Eletrónicas.

CAPÍTULO III
REGIME SANCIONATÓRIO

Artigo 14.º Contraordenação
1. Constitui contraordenação punível com a coima mínima de € 1500 e máxima de € 25 000, quando praticada por pessoas singulares, e com coima mínima de € 5000 e máxima de € 5 000 000, quando praticada por pessoas coletivas:
a) A inobservância das regras de segurança das redes impostas pelos n.ºs 1, 2, 3 e 10 do artigo 3.º;

b) A inobservância das regras de segurança no tratamento de dados pessoais impostas pelo n.º 9 do artigo 3.º;

c) A violação das obrigações estabelecidas nos n.ºs 1, 2, 3, 4, 5 e 10 do artigo 3.º-A ou determinadas nos termos previstos nos respetivos n.ºs 6 e 9;

d) A violação da obrigação estabelecida no n.º 1 do artigo 4.º, da proibição estabelecida no n.º 2 do artigo 4.º e a realização de gravações em desrespeito do n.º 3 do artigo 4.º;

e) A inobservância das condições de armazenamento e acesso à informação previstas no artigo 5.º;

f) O envio de comunicações para fins de marketing direto em violação dos n.ºs 1 e 2 do artigo 13.º-A;

g) A violação das obrigações impostas no n.º 3 do artigo 13.º-A;

h) O envio de correio eletrónico em violação do n.º 4 do artigo 13.º-A;

i) A violação da obrigação estabelecida no n.º 1 do artigo 13.º-B;

j) A violação do disposto no n.º 3 do artigo 13.º-B pelas entidades previstas no respetivo n.º 1;

k) A violação da obrigação de prestação de informações estabelecida no artigo 13.º-E;

l) O incumprimento de ordens ou deliberações da CNPD, emitidas nos termos do artigo 13.º-D e regularmente comunicadas aos seus destinatários;

m) O incumprimento de ordens ou deliberações do ICP-ANACOM, emitidas nos termos do artigo 13.º-D e regularmente comunicadas aos seus destinatários.

2. Constitui contraordenação punível com a coima mínima de € 500 e máxima de € 20 000, quando praticada por pessoas singulares, e com coima mínima de € 2500 e máxima de € 2 500 000, quando praticada por pessoas coletivas:
a) A violação dos requisitos de notificação previstos nos n.ºs 7, 8 e 10 do artigo 3.º-A ou determinados nos termos previstos no respetivo n.º 9;

b) A inobservância das condições de tratamento e armazenamento de dados de tráfego e de dados de localização previstas nos artigos 6.º e 7.º;

c) A violação das obrigações previstas nos n.ºs 1, 2 e 4 do artigo 8.º e nos artigos 9.º e 11.º;

d) A violação das obrigações previstas no artigo 10.º;

e) A violação do disposto no artigo 13.º

3. Quer a contraordenação consista no incumprimento de um dever legal quer no incumprimento de uma ordem ou deliberação emanada da CNPD ou do ICP-ANACOM, nas respetivas áreas de competência, a aplicação e o cumprimento das sanções não dispensam o infrator do cumprimento, se este ainda for possível.

4. A CNPD ou o ICP-ANACOM, nas respetivas áreas de competência, podem ordenar ao infrator que cumpra o dever ou ordem em causa, sob pena de sanção pecuniária compulsória nos termos do artigo 15.º-C.

5. A negligência e a tentativa são puníveis, sendo os limites mínimos e máximos da coima reduzidos a metade.

Artigo 15.º Processamento e aplicação de coimas
1. Compete à CNPD a instauração, instrução e arquivamento de processos de contraordenação, bem como a aplicação de admoestações, coimas e sanções acessórias, por violação do disposto no n.º 9 do artigo 3.º, no artigo 3.º-A, no n.º 3 do artigo 4.º, nos artigos 5.º, 6.º e 7.º, nos n.os 1, 2 e 4 do artigo 8.º, no artigo 10.º, no artigo 13.º, nos n.os 1 a 4 do artigo 13.º-A, nos n.os 1 e 3 do artigo 13.º-B e na alínea l) do n.º 1 do artigo 14.º

2. Compete ao ICP-ANACOM a instauração, instrução e arquivamento de processos de contraordenação, bem como a aplicação de admoestações, coimas e sanções acessórias, por violação do disposto nos n.os 1, 2, 3 e 10 do artigo 3.º, nos n.os 1 e 2 do artigo 4.º, no artigo 9.º, no artigo 11.º, no artigo 13.º-E e na alínea m) do n.º 1 do artigo 14.º

3. A instauração de processos de contraordenação e a respetiva aplicação de coimas relativos aos ilícitos previstos no número anterior são da competência do conselho de administração do ICP-ANACOM, cabendo a instrução aos respetivos serviços.

4. As competências previstas no número anterior podem ser delegadas.

5. O montante das coimas reverte para o Estado em 60 % e para a CNPD ou para o ICP-ANACOM, consoante os casos, em 40 %.

Artigo 15.º-A Sanções acessórias
1. No âmbito das contraordenações previstas no n.º 2 do artigo 15.º, sempre que a gravidade da infração e a culpa do agente o justifique, o ICP-ANACOM pode aplicar uma sanção acessória de perda a favor do Estado de objetos, equipamentos e dispositivos ilícitos, incluindo o produto do benefício obtido pelo infrator através da prática da contraordenação.

2. Quem desrespeitar uma sanção acessória que lhe tenha sido aplicada, incorre em crime de desobediência qualificada.

Artigo 15.º-B Perda a favor do Estado
1. Sem prejuízo do disposto no n.º 1 do artigo anterior, consideram-se perdidos a favor do Estado os objetos, equipamentos e dispositivos ilícitos que tenham sido cautelar ou provisoriamente apreendidos pelo ICP-ANACOM e que, após notificação aos interessados para que os recolham, não tenham sido reclamados no prazo de 60 dias.

2. Os objetos, equipamentos e dispositivos ilícitos perdidos a favor do Estado revertem para o ICP-ANACOM, que lhes dará o destino que julgar adequado.

Artigo 15.º-C Sanções pecuniárias compulsórias
1. Sem prejuízo de outras sanções aplicáveis, em caso de incumprimento de decisões da CNPD ou do ICP-ANACOM que imponham sanções administrativas ou ordenem, no exercício dos poderes que legalmente lhes assistem, a adoção de comportamentos ou de medidas determinadas aos destinatários da presente lei, podem aquelas autoridades, fundamentadamente, impor uma sanção pecuniária compulsória, nos casos referidos nos n.^{os} 1, 3, 4 e 5 do artigo 10.º, nos n.^{os} 1, 3, e 4 do artigo 13.º e nas alíneas a) a i), j) e l) a m) do n.º 1 e a), b), c), d) e e) do n.º 2 do artigo 14.º

2. A sanção pecuniária compulsória consiste na imposição ao seu destinatário do pagamento de uma quantia pecuniária por cada dia de atraso no cumprimento para além do prazo nela fixado.

3. A sanção compulsória é fixada segundo critérios de razoabilidade e proporcionalidade, atendendo à situação económica do infrator, designadamente ao seu volume de negócios no ano civil anterior, e ao impacto negativo do incumprimento no mercado e nos utilizadores, podendo o montante diário situar-se entre € 500 e € 100 000.

4. Os montantes fixados nos termos do número anterior podem ser variáveis para cada dia de incumprimento, num sentido crescente, não podendo ultrapassar o montante máximo de € 3 000 000 nem a duração máxima de 30 dias.

5. O montante da sanção aplicada reverte para o Estado em 60 % e para a CNPD ou para o ICP-ANACOM em 40 %.

6. Dos atos da CNPD e do ICP-ANACOM, praticados ao abrigo do presente artigo, cabe recurso, consoante sejam praticados no âmbito de um processo de contraordenação ou administrativo, nos termos da legislação aplicável a cada tipo de processo em causa.

Artigo 16.º Legislação subsidiária
Em tudo o que não esteja previsto na presente lei, são aplicáveis as disposições sancionatórias que constam dos artigos 33.º a 39.º da Lei da Proteção de Dados Pessoais.

CAPÍTULO IV
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Artigo 17.º Características técnicas e normalização
1. O cumprimento do disposto na presente lei não deve determinar a imposição de requisitos técnicos específicos dos equipamentos terminais ou de outros equipamentos de comunicações eletrónicas que possam impedir a colocação no mercado e a circulação desses equipamentos nos países da União Europeia.

2. Excetua-se do disposto no número anterior a elaboração e emissão de características técnicas específicas necessárias à execução da presente lei, as quais devem ser comunicadas à Comissão Europeia nos termos dos procedimentos previstos no Decreto-Lei n.º 58/2000, de 18 de Abril.

Artigo 18.º Disposições transitórias
1. O disposto no artigo 13.º não é aplicável às edições de listas já elaboradas ou colocadas no mercado, em formato impresso ou eletrónico fora de linha, antes da entrada em vigor da presente lei.

2. No caso de os dados pessoais dos assinantes de serviços telefónicos acessíveis ao público fixos ou móveis terem sido incluídos numa lista pública de assinantes, em conformidade com a legislação anterior e antes da entrada em vigor da presente lei, os dados pessoais desses assinantes podem manter-se nessa lista pública nas suas versões impressa ou eletrónica.

3. No caso previsto no número anterior, os assinantes têm o direito de decidir pela retirada dos seus dados pessoais da lista pública em causa, devendo receber previamente informação completa sobre as finalidades e opções da mesma em conformidade com o artigo 13.º

4. A informação referida no número anterior deve ser enviada aos assinantes no prazo máximo de seis meses a contar da data de entrada em vigor da presente lei.

Artigo 19.º Revogação
É revogada a Lei n.º 69/98, de 28 de Outubro.

Artigo 20.º Entrada em vigor
A presente lei entra em vigor no dia seguinte ao da sua publicação.

Aprovada em 1 de Julho de 2004.
O Presidente da Assembleia da República,
João Bosco Mota Amaral.
Promulgada em 2 de Agosto de 2004.
Publique-se.
O Presidente da República,
JORGE SAMPAIO.
Referendada em 5 de Agosto de 2004.
O Primeiro-Ministro,
Pedro Miguel de Santana Lopes.

14. Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[56]

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia e, nomeadamente, o seu artigo 95.º,

Tendo em conta a proposta da Comissão[57],

Tendo em conta o parecer do Comité Económico e Social[58],

Após consulta ao Comité das Regiões,

Deliberando nos termos do artigo 251.º do Tratado[59],

Considerando o seguinte:

1 // A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[60], exige dos Estados-Membros que garantam os direitos e liberdades das pessoas singulares no que respeita ao tratamento de dados pessoais, nomeadamente o seu direito à privacidade, com o objetivo de assegurar a livre circulação de dados pessoais na Comunidade.

---

[56] Última modificação legislativa: Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009 que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) nº 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor

[57] JO C 365 E de 19.12.2000, p. 233.

[58] JO C 123 de 25.4.2001, p. 53.

[59] Parecer do Parlamento Europeu de 13 de Novembro de 2001 (ainda não publicado no Jornal Oficial), posição comum do Conselho de 28 de Janeiro de 2002 (JO C 113 E de 14.5.2002, p. 39) e decisão do Parlamento Europeu de 30 de Maio de 2002 (ainda não publicada no Jornal Oficial). Decisão do Conselho de 25 de Junho de 2002.

[60] JO L 281 de 23.11.1995, p. 31.

2 // A presente diretiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Europeia. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º e 8.º da citada carta.

3 // A confidencialidade das comunicações está garantida nos termos dos instrumentos internacionais relativos aos direitos humanos, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, e as Constituições dos Estados-Membros.

4 // A Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações[61], transpôs os princípios estabelecidos na Diretiva 95/46/CE em regras específicas para o sector das telecomunicações. A Diretiva 97/66/CE deve ser adaptada ao desenvolvimento dos mercados e das tecnologias dos serviços de comunicações eletrónicas, de modo a proporcionar um nível idêntico de proteção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas. Essa diretiva deve, portanto, ser revogada e substituída pela presente diretiva.

5 // Estão a ser introduzidas nas redes de comunicações públicas da Comunidade novas tecnologias digitais avançadas, que suscitam requisitos específicos de proteção de dados pessoais e da privacidade do utilizador. O desenvolvimento da sociedade da informação caracteriza-se pela introdução de novos serviços de comunicações eletrónicas. O acesso a redes móveis digitais está disponível a custos razoáveis para um vasto público. Essas redes digitais têm grandes capacidades e possibilidades de tratamento de dados pessoais. O desenvolvimento transfronteiriço bem sucedido desses serviços depende em parte da confiança dos utilizadores na garantia da sua privacidade.

6 // A internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infraestrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações eletrónicas. Os serviços de comunicações eletrónicas publicamente disponíveis através da internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade.

---

[61] *JO L 24 de 30.1.1998, p. 1.*

7 // No caso das redes de comunicações públicas, é necessário estabelecer disposições legislativas, regulamentares e técnicas específicas para a proteção dos direitos e liberdades fundamentais das pessoas singulares e dos interesses legítimos das pessoas coletivas, em especial no que respeita à capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores.

8 // As disposições legislativas, regulamentares e técnicas aprovadas pelos Estados-Membros em matéria de proteção dos dados pessoais, da privacidade e dos interesses legítimos das pessoas coletivas no sector das comunicações eletrónicas, devem ser harmonizadas, por forma a evitar obstáculos ao mercado interno das comunicações eletrónicas, em consonância com o disposto no artigo 14.º do Tratado. A harmonização deve limitar-se aos requisitos necessários para que a promoção e o desenvolvimento de novos serviços e redes de comunicações eletrónicas entre Estados-Membros não sejam prejudicados.

9 // Os Estados-Membros, os prestadores e os utilizadores em questão, juntamente com as instâncias comunitárias competentes, devem cooperar no estabelecimento e desenvolvimento das tecnologias pertinentes, sempre que tal seja necessário para aplicar as garantias previstas na presente diretiva, tendo especialmente em conta os objetivos de reduzir ao mínimo o tratamento de dados pessoais e de utilizar dados anónimos ou pseudónimos, sempre que possível.

10 // No sector das comunicações eletrónicas, é aplicável a Diretiva 95/46/CE, especialmente no que se refere a todas as questões relacionadas com a proteção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente diretiva, incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares. A Diretiva 95/46/CE é aplicável aos serviços de comunicações não acessíveis ao público.

11 // Tal como a Diretiva 95/46/CE, a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades não reguladas pelo direito comunitário. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.º 1 do artigo 15.º da presente diretiva, necessários para

a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

12 // Os assinantes de um serviço de comunicações eletrónicas publicamente disponível podem ser pessoas singulares ou coletivas. Em complemento da Diretiva 95/46/CE, a presente diretiva destina-se a proteger os direitos fundamentais das pessoas singulares, nomeadamente o seu direito à privacidade, bem como os interesses legítimos das pessoas coletivas. A presente diretiva não implica a obrigação, para os Estados-Membros, de tornarem a aplicação da Diretiva 95/46/CE extensiva à proteção dos interesses legítimos das pessoas coletivas, que está assegurada no âmbito da legislação comunitária e nacional nesta matéria.

13 // A relação contratual entre um assinante e um prestador de serviços pode implicar um pagamento periódico ou único pelo serviço prestado ou a prestar. Os cartões pré-pagos são também considerados um contrato.

14 // Os dados de localização podem incidir sobre a latitude, a longitude e a altitude do equipamento terminal do utilizador, sobre a direção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização.

15 // Uma comunicação pode incluir qualquer informação relativa a nomes, números ou endereços fornecida pelo remetente de uma comunicação ou pelo utilizador de uma ligação para efetuar a comunicação. Os dados

de tráfego podem incluir qualquer tradução desta informação pela rede através da qual a comunicação é transmitida, para efeitos de execução da transmissão. Os dados de tráfego podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação. Podem igualmente consistir no formato em que a comunicação é enviada pela rede.

16 // As informações enviadas no âmbito de um serviço de difusão prestado através de uma rede pública de comunicações destinam-se a uma audiência potencialmente ilimitada e não constituem uma comunicação na aceção da presente diretiva. No entanto, nos casos em que é possível identificar o assinante ou utilizador que recebe as informações em causa, como o dos serviços de vídeo-a-pedido, as informações enviadas constituem uma comunicação na aceção da presente diretiva.

17 // Para efeitos da presente diretiva, o consentimento por parte do utilizador ou assinante, independentemente de este ser uma pessoa singular ou coletiva, deve ter a mesma aceção que o consentimento da pessoa a quem os dados dizem respeito conforme definido e especificado na Diretiva 95/46/CE. O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na internet.

18 // Constituem serviços de valor acrescentado, por exemplo, os conselhos sobre as tarifas menos dispendiosas, a orientação rodoviária, as informações sobre o trânsito, as previsões meteorológicas e a informação turística.

19 // A aplicação de determinados requisitos relacionados com a apresentação e restrição da linha chamadora e da linha conectada e com o reencaminhamento automático de chamadas para as linhas de assinante ligadas a centrais analógicas não deve ser obrigatória em casos específicos, quando se verifique que essa aplicação é tecnicamente impossível ou impõe um esforço económico desproporcionado. É importante para as partes interessadas serem informadas desses casos, devendo os Estados-Membros notificá-los à Comissão.

20 // Os prestadores de serviços devem tomar medidas adequadas para garantir a segurança dos seus serviços, se necessário em conjunto com o fornecedor da rede, e informar os assinantes sobre quaisquer riscos específicos de violação da segurança da rede. Esses riscos podem ocorrer especialmente para os serviços de comunicações eletrónicas através de uma rede aberta como a internet ou a telefonia móvel analógica. É particularmente importante para os assinantes e utilizadores desses serviços receberem do seu prestador de serviços todas as informações acerca dos riscos existentes em termos de segurança para os quais o prestador de serviços em causa não dispõe de soluções. Os fornecedores de serviços que disponibilizam serviços de comunicações eletrónicas publicamente disponíveis através da internet devem informar os seus utilizadores e assinantes das medidas que podem tomar para proteger a segurança das suas comunicações, como seja o recurso a tipos específicos de software ou tecnologias de cifra. O requisito de informar os assinantes dos riscos de segurança específicos não isenta os fornecedores de serviços da obrigação de, a expensas suas, adotarem as necessárias medidas imediatas para remediar quaisquer riscos novos e imprevistos e restabelecer o nível normal de segurança do serviço. A prestação de informações ao assinante sobre os riscos de segurança deverá ser gratuita, com exceção dos custos nominais eventualmente incorridos pelo assinante ao receber ou recolher as informações através, por exemplo, do descarregamento de uma mensagem de correio eletrónico. A segurança é avaliada em função do disposto no artigo 17.º da Diretiva 95/46/CE.

21 // Devem ser tomadas medidas para impedir o acesso não autorizado às comunicações efetuadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis, a fim de proteger a confidencialidade do seu conteúdo e de quaisquer dados com elas relacionados. A legislação nacional de alguns Estados-Membros apenas proíbe o acesso intencional não autorizado às comunicações.

22 // A proibição de armazenamento das comunicações e dos dados de tráfego a elas relativos por terceiros que não os utilizadores ou sem o seu consentimento não tem por objetivo proibir qualquer armazenamento automático, intermédio e transitório de informações, desde que esse armazenamento se efetue com o propósito exclusivo de realizar a transmissão através da rede de comunicação eletrónica e desde que as informações não sejam armazenadas por um período de

tempo superior ao necessário para a transmissão e para fins de gestão de tráfego e que durante o período de armazenamento se encontre garantida a confidencialidade das informações. Sempre que tal se torne necessário para tornar mais eficiente o reenvio de informações acessíveis publicamente a outros destinatários do serviço, a seu pedido, a presente diretiva não deve impedir que as informações em causa possam continuar armazenadas, desde que as mesmas sejam, de qualquer modo, acessíveis ao público sem restrições e na condição de serem eliminados os dados relativos aos assinantes ou utilizadores que o solicitem.

23 // A confidencialidade das comunicações deve igualmente ser assegurada no âmbito de práticas comerciais lícitas. Sempre que tal seja necessário e legalmente autorizado, as comunicações poderão ser gravadas para o efeito de constituir prova de uma transação comercial. A este tratamento é aplicável o disposto na Diretiva 95/46/CE. As partes nas comunicações deverão ser previamente informadas da gravação, do seu objetivo e da duração do seu armazenamento. A comunicação registada deve ser eliminada o mais rapidamente possível e, em todo o caso, o mais tardar até ao termo do período em que a transação pode ser legalmente impugnada.

24 // O equipamento terminal dos utilizadores de redes de comunicações eletrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais. Os denominados «gráficos espiões», «programas-espiões», («*spyware*»), «gráficos-espiões» («*web bugs*») e «identificadores ocultos» («*hidden identifiers*») e outros dispositivos análogos podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das atividades do utilizador e podem constituir uma grave intrusão na privacidade desses utilizadores. A utilização desses dispositivos deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa.

25 // Todavia, esses dispositivos, por exemplo os denominados testemunhos de conexão («cookies»), podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da conceção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transações em linha. Sempre que esses dispositivos, por exemplo os

testemunhos de conexão («cookies»), se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Diretiva 95/46/CE, acerca da finalidade dos testemunhos de conexão («cookies») ou dos dispositivos análogos por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam. Os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal. Tal é particularmente importante nos casos em que outros utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento. A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio web específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão («cookie») ou dispositivo análogo, caso seja utilizado para um fim legítimo.

26 // Os dados relativos aos assinantes tratados em redes de comunicações eletrónicas para estabelecer ligações e para transmitir informações contêm informações sobre a vida privada das pessoas singulares e incidem no direito ao sigilo da sua correspondência ou incidem nos legítimos interesses das pessoas coletivas. Esses dados apenas podem ser armazenados na medida do necessário para a prestação do serviço, para efeitos de faturação e de pagamentos de interligação, e por um período limitado. Qualquer outro tratamento desses dados que o prestador de serviços de comunicações eletrónicas publicamente disponíveis possa querer efetuar para a comercialização dos seus próprios serviços de comunicações eletrónicas, ou para a prestação de serviços de valor acrescentado, só é permitido se o assinante tiver dado o seu acordo, com base nas informações exatas e completas que o prestador de serviços de comunicações eletrónicas publicamente disponíveis lhe tiver comunicado

relativamente aos tipos de tratamento posterior que pretenda efetuar e sobre o direito do assinante de não dar ou retirar o seu consentimento a esse tratamento. Os dados de tráfego utilizados para comercialização de serviços de comunicações ou para a prestação de serviços de valor acrescentado devem igualmente ser eliminados ou tornados anónimos após o fornecimento do serviço. Os prestadores de serviços devem informar sempre os assinantes acerca dos tipos de dados que estão a tratar e dos fins e duração desse tratamento.

27 // O momento exato da conclusão da transmissão de uma comunicação, após o qual os dados de tráfego devem ser eliminados, a não ser para efeitos de faturação, pode depender do tipo de serviço de comunicações eletrónicas prestado. Por exemplo, tratando-se de uma chamada de telefonia vocal, a transmissão estará concluída logo que um dos utilizadores termine a ligação e, no que se refere ao correio eletrónico, a transmissão é concluída assim que o destinatário recolhe a mensagem, normalmente a partir do servidor do seu prestador de serviços.

28 // A obrigação de eliminar ou tornar anónimos os dados de tráfego quando deixem de ser necessários para efeitos da transmissão da comunicação não é incompatível com os procedimentos utilizados na internet, tais como a memorização de endereços IP no Sistema de Nomes de Domínios ou a memorização de endereços IP ligados a um endereço físico, ou ainda a utilização de informações de entrada no sistema para controlar o direito de acesso a redes ou serviços.

29 // O prestador de serviços pode tratar dados de tráfego relativos a assinantes e utilizadores, sempre que necessário em casos específicos, para detetar falhas técnicas ou erros na transmissão das comunicações. Os dados de tráfego necessários para efeitos de faturação podem também ser tratados pelo prestador de serviços para detetar e fazer cessar a fraude que consiste na utilização não paga do serviço de comunicação.

30 // Os sistemas de fornecimento de redes e serviços de comunicações eletrónicas devem ser concebidos de modo a limitar ao mínimo o volume necessário de dados pessoais. Todas as atividades ligadas à prestação do serviço de comunicações eletrónicas que ultrapassem a transmissão e faturação de uma comunicação deverão basear-se em dados de tráfego agregados impossíveis de associar a assinantes ou utilizadores. Sempre

que não possam basear-se em dados agregados, essas atividades devem ser equiparadas a serviços de valor acrescentado que requerem o consentimento do assinante.

31 // O consentimento necessário ao tratamento de dados pessoais, tendo em vista a prestação de um determinado serviço de valor acrescentado, terá de ser dado quer pelo utilizador, quer pelo assinante, consoante os dados a tratar e o tipo de serviço a prestar, e conforme seja ou não possível, em termos técnicos, processuais e contratuais, estabelecer uma distinção entre o indivíduo que utiliza o serviço de comunicações eletrónicas e a pessoa singular ou coletiva que fez a respetiva assinatura.

32 // Sempre que o prestador de um serviço de comunicações eletrónicas ou de um serviço de valor acrescentado proceda à subcontratação de outra entidade para o tratamento dos dados pessoais necessário à prestação desses serviços, essa subcontratação e o subsequente tratamento de dados terão de obedecer inteiramente aos requisitos aplicáveis aos responsáveis pelo tratamento dos dados e respetivos subcontratantes nos termos da Diretiva 95/46/CE. Sempre que a prestação de um serviço de valor acrescentado exija o reenvio de dados de tráfego ou de localização por um prestador de serviços de comunicações eletrónicas a um prestador de serviços de valor acrescentado, os assinantes ou utilizadores a quem os dados dizem respeito devem também ser inteiramente informados desse reenvio antes de darem o seu consentimento quanto ao tratamento dos dados.

33 // A introdução de faturação detalhada melhorou as possibilidades de o assinante verificar a exatidão dos montantes cobrados pelo prestador do serviço, embora possa, ao mesmo tempo, pôr em causa a privacidade dos utilizadores de serviços de comunicações eletrónicas publicamente disponíveis. Por conseguinte, para preservar a privacidade do utilizador, os Estados-Membros devem incentivar o desenvolvimento de opções de serviços de comunicações eletrónicas, tais como possibilidades de pagamento alternativas que permitam o acesso anónimo ou estritamente privado a serviços de comunicações eletrónicas publicamente disponíveis, como a utilização de cartões telefónicos e a possibilidade de pagamento por cartão de crédito. Para o mesmo efeito, os Estados-Membros podem solicitar aos operadores que ofereçam aos seus assinantes um tipo diferente de faturação detalhada em que sejam suprimidos alguns dos algarismos do número para o qual é feita a chamada.

34 // No que respeita à identificação da linha chamadora, é necessário proteger o direito da parte que efetua a chamada de suprimir a apresentação da identificação da linha da qual a chamada é feita e o direito da parte chamada de rejeitar chamadas de linhas não identificadas. Em casos específicos, justifica-se anular a supressão da apresentação da identificação da linha chamadora. Certos assinantes, em especial os serviços de linhas SOS e outras organizações similares, têm interesse em garantir o anonimato de quem faz as chamadas. É necessário, no que se refere à identificação da linha conectada, proteger o direito e os legítimos interesses da parte chamada de impedir a apresentação da identificação da linha à qual a parte chamadora se encontra efetivamente ligada, em especial no caso das chamadas reencaminhadas. Os prestadores de serviços de comunicações eletrónicas publicamente disponíveis devem informar os seus assinantes da existência da identificação da linha chamadora e conectada na rede, de todos os serviços que são oferecidos com base na identificação da linha chamadora e conectada e das opções de privacidade existentes. Tal permitirá aos assinantes fazer uma escolha informada sobre os recursos de protecção da privacidade que possam querer utilizar. As opções de privacidade que são oferecidas linha a linha não devem necessariamente estar disponíveis como um serviço automático da rede, mas podem ser obtidas através de um simples pedido ao prestador do serviço de comunicações eletrónicas publicamente disponível.

35 // Nas redes móveis digitais, os dados de localização que fornecem a posição geográfica do equipamento terminal do seu utilizador móvel são tratados para permitir a transmissão das comunicações. Esses dados são dados de tráfego, abrangidos pelo disposto no artigo 6.º da presente diretiva. No entanto, as redes móveis digitais podem ainda ter a capacidade de tratar dados de localização que são mais precisos do que o necessário para a transmissão de comunicações e que são utilizados para a prestação de serviços de valor acrescentado, tais como serviços que prestam aos condutores informações e orientações individualizadas sobre o tráfego. O tratamento desses dados para serviços de valor acrescentado apenas deve ser permitido se os assinantes tiverem dado o seu consentimento. Mesmo nos casos em que os assinantes tenham dado o seu consentimento, deverão dispor de um meio simples e gratuito de recusar temporariamente o tratamento de dados de localização.

36 // Os Estados-Membros podem restringir os direitos à privacidade dos utilizadores e dos assinantes no que respeita à identificação da linha chamadora, sempre que tal for necessário para detetar chamadas inoportunas e, no que respeita à identificação da linha chamadora, aos dados de localização, sempre que tal seja necessário para possibilitar que os serviços de emergência desempenhem as suas missões de forma tão eficaz quanto possível. Para esses efeitos, os Estados-Membros podem aprovar disposições específicas que permitam que os prestadores de serviços de comunicações eletrónicas facultem o acesso à identificação da linha chamadora e aos dados referentes à localização sem o consentimento prévio dos utilizadores ou assinantes em causa.

37 // Devem prever-se medidas de proteção dos assinantes contra os incómodos que possam ser provocados pelo reencaminhamento automático de chamadas por terceiros. Além disso, nesses casos, deve ser possível aos assinantes, mediante simples pedido ao prestador do serviço de comunicações eletrónicas publicamente disponível, interromper o reencaminhamento das que são passadas para os seus terminais.

38 // As listas de assinantes de serviços de comunicações eletrónicas são amplamente distribuídas e públicas. O direito à privacidade das pessoas singulares e os legítimos interesses das pessoas coletivas exigem que os assinantes possam determinar se os seus dados pessoais devem ser publicados numa lista e, nesta eventualidade, quais os dados a incluir. Os fornecedores de listas públicas devem informar os assinantes que vão ser incluídos nessas listas dos fins a que se destina a lista e de qualquer utilização particular que possa ser feita de versões eletrónicas de listas públicas, especialmente através de funções de procura incorporadas no software, tais como funções de procura invertida que permitam aos utilizadores descobrir o nome e o endereço do assinante apenas com base no número de telefone.

39 // A obrigação de informar os assinantes do fim ou fins a que se destinam as listas públicas em que vão ser incluídos os seus dados pessoais deverá caber à parte que recolhe os dados tendo em vista essa inclusão. Nos casos em que os dados possam ser transmitidos a um ou mais terceiros, o assinante deverá ser informado desta possibilidade e do destinatário ou das categorias de possíveis destinatários. Qualquer transmissão deve obedecer à condição de que os dados não possam ser

utilizados para outros fins diferentes dos que motivaram a sua recolha. Se a parte que recolhe os dados a partir do assinante ou de terceiros a quem os mesmos tenham sido transmitidos pretender utilizá-los para outro fim, quer a parte que recolheu os dados, quer o terceiro a quem foram transmitidos, terá de obter novo consentimento do assinante.

40 // Devem ser previstas medidas de proteção dos assinantes contra a invasão da sua privacidade através de chamadas não solicitadas para fins de comercialização direta, em especial através de aparelhos de chamadas automáticas, aparelhos de fax e de correio eletrónico, incluindo mensagens SMS. Essas formas de comunicações comerciais não solicitadas podem, por um lado, ser relativamente baratas e fáceis de efetuar e, por outro, acarretar um ónus e/ou custo ao destinatário. Além disso, em certos casos o seu volume pode também provocar dificuldades às redes de comunicações eletrónicas e ao equipamento terminal. No que diz respeito a essas formas de comunicações não solicitadas para fins de comercialização direta, justifica-se que se obtenha, antes de essas comunicações serem enviadas aos destinatários, o seu consentimento prévio e explícito. O mercado único exige uma abordagem harmonizada para assegurar, a nível da Comunidade, regras simples para o comércio e os utilizadores.

41 // No contexto de uma relação comercial existente, é razoável permitir a utilização de coordenadas eletrónicas do contacto para a oferta de produtos ou serviços análogos, mas apenas por parte da mesma empresa que obteve os elementos da comunicação junto do cliente em conformidade com a Diretiva 95/46/CE. Sempre que sejam obtidas coordenadas eletrónicas do contacto, o cliente deverá ser informado de forma clara e distinta sobre a sua futura utilização para fins de comercialização direta, e deve-lhe ser dada a oportunidade de recusar essa utilização. Deverá continuar a ser-lhe dada gratuitamente essa oportunidade em todas as subsequentes mensagens de comercialização direta, exceto no que diz respeito a eventuais custos para a transmissão dessa recusa.

42 // Outras formas de comercialização direta que são mais dispendiosas para a entidade que a envia e que não acarretam quaisquer custos financeiros para os assinantes e utilizadores, como por exemplo chamadas de telefonia vocal personalizadas, podem justificar a manutenção de um

sistema que dê aos assinantes ou utilizadores a possibilidade de indicarem que não pretendem receber essas chamadas. Todavia, a fim de não diminuir os atuais níveis de proteção da privacidade, os Estados-Membros deverão ser autorizados a manter os sistemas nacionais, só permitindo essas chamadas aos assinantes e utilizadores que tenham previamente dado o seu consentimento.

43 // A fim de facilitar uma aplicação eficaz das regras comunitárias relativas às mensagens não solicitadas para fins de comercialização direta, é necessário proibir a utilização de falsas identidades ou de falsos endereços ou números quando se enviam mensagens não solicitadas para fins de comercialização direta.

44 // Determinados sistemas de correio eletrónico permitem aos assinantes visualizar a referência do remetente e do assunto das mensagens de correio eletrónico e suprimi-las sem terem de carregar o resto do conteúdo da mensagem ou os anexos, reduzindo assim os custos que poderiam decorrer de descarregar mensagens de correio eletrónico ou anexos não solicitados. Estas modalidades de funcionamento podem continuar a ser úteis em determinados casos, como instrumento complementar às obrigações gerais estabelecidas na presente diretiva.

45 // A presente diretiva não prejudica as disposições tomadas pelos Estados-Membros para proteger os interesses legítimos das pessoas coletivas no tocante às comunicações não solicitadas para efeitos de comercialização direta. No caso dos Estados-Membros que estabeleçam um registo de autoexclusão relativo a esse tipo de comunicações para as pessoas coletivas, na sua maior parte utilizadores comerciais, aplicam-se integralmente as disposições do artigo 7.º da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (diretiva sobre o comércio eletrónico)[62].

46 // As funcionalidades para a prestação de serviços de comunicações eletrónicas podem ser integradas na rede ou em qualquer parte do equipamento terminal do utilizador, incluindo o software. A proteção

[62] *JO L 178 de 17.7.2000, p. 1.*

dos dados pessoais e da privacidade do utilizador de serviços de comunicações eletrónicas publicamente disponíveis deve ser independente da configuração dos vários componentes necessários para prestar o serviço e da distribuição das funcionalidades necessárias entre esses componentes. A Diretiva 95/46/CE abrange todas as formas de tratamento de dados pessoais, independentemente da tecnologia utilizada. A existência de regras específicas para os serviços de comunicações eletrónicas em paralelo com regras gerais aplicáveis a outros elementos necessários para a prestação desses serviços pode não facilitar a proteção dos dados pessoais e da privacidade de um modo tecnologicamente neutro. Por conseguinte, pode ser necessário adotar medidas que exijam que os fabricantes de certos tipos de equipamentos utilizados para serviços de comunicações eletrónicas construam os seus produtos de tal modo que incorporem salvaguardas para garantir que os dados pessoais e a privacidade do utilizador ou assinante sejam protegidos. A adoção dessas medidas nos termos da Diretiva 1999/5/CE do Parlamento Europeu e do Conselho, de 9 de Março de 1999, relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade[63], garantirá que a introdução de características técnicas nos equipamentos de comunicações eletrónicas, incluindo software, para efeitos de proteção dos dados, seja harmonizada com vista à realização do mercado interno.

47 // A legislação nacional deve prever a possibilidade de ações judiciais, em caso de desrespeito dos direitos dos utilizadores e dos assinantes. Devem ser impostas sanções a qualquer pessoa que, quer esteja sujeita ao direito privado ou público, não cumpra as medidas nacionais adotadas ao abrigo da presente diretiva.

48 // Na aplicação da presente diretiva, é útil recorrer à experiência do grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, constituído por representantes das autoridades de fiscalização dos Estados-Membros, previsto no artigo 29.º da Diretiva 95/46/CE.

49 // Para facilitar o cumprimento da presente diretiva, são necessárias determinadas adaptações específicas para o processamento de dados já em curso à data da entrada em vigor das disposições nacionais de transposição da presente diretiva,

---

[63] JO L 91 de 7.4.1999, p. 10.

ADOTARAM A PRESENTE DIRECTIVA:

Artigo 1.º Âmbito e objetivos
1. A presente diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade.

2. Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

3. A presente diretiva não é aplicável a atividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.

Artigo 2.º Definições
Salvo disposição em contrário, são aplicáveis as definições constantes da Diretiva 95/46/CE e da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro)[64].

São também aplicáveis as seguintes definições:
a) «Utilizador» é qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

b) «Dados de tráfego» são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma;

[64] *JO L 108 de 24.4.2002, p. 33.*

c) «Dados de localização», quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

d) «Comunicação» é qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível; não se incluem aqui as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações eletrónicas, exceto na medida em que a informação possa ser relacionada com o assinante ou utilizador identificável que recebe a informação;

e) (revogado)

f) «Consentimento» por parte do utilizador ou assinante significa o consentimento dado pela pessoa a quem dizem respeito os dados, previsto na Diretiva 95/46/CE;

g) «Serviço de valor acrescentado» é qualquer serviço que requeira o tratamento de dados de tráfego ou dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma;

h) «Correio eletrónico» é qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher.

i) «Violação de dados pessoais», uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público na Comunidade.

Artigo 3.º Serviços abrangidos
A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na Comunidade,

nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação.

Artigo 4.º Segurança do processamento
1. O prestador de um serviço de comunicações eletrónicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes.

1.-A. Sem prejuízo do disposto na Diretiva 95/46/CE, as medidas referidas no n.º 1 compreendem, no mínimo:
- a garantia de que aos dados pessoais apenas possa ter acesso pessoal autorizado, para fins autorizados a nível legal,
- a proteção dos dados pessoais armazenados ou transmitidos contra a destruição acidental ou ilegal, a perda ou alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizados ou ilegais, e
- a garantia da aplicação de uma política de segurança relativa ao tratamento dos dados pessoais.
As autoridades nacionais competentes devem ter competência para auditar as medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar.

2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações eletrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.

3. No caso de violação de dados pessoais, o prestador dos serviços de comunicações eletrónicas acessíveis ao público comunica, sem atraso injustificado, a violação à autoridade nacional competente.
Caso a violação de dados pessoais possa afetar negativamente os dados pessoais e a privacidade do assinante ou de um indivíduo, o prestador

notifica essa violação ao assinante ou ao indivíduo sem atraso injustificado. A notificação de uma violação de dados pessoais a um assinante ou outra pessoa afetada não é exigida se a autoridade competente considerar que o prestador provou cabalmente que tomou as medidas tecnológicas de proteção adequadas e que essas medidas foram aplicadas aos dados a que diz respeito a violação. Essas medidas tecnológicas de proteção devem tornar os dados incompreensíveis para todas as pessoas que não estejam autorizadas a aceder a esses dados.
Sem prejuízo da obrigação que incumbe ao prestador de notificar os assinantes e as pessoas afetadas, se este comunicar ao assinante ou ao indivíduo a violação dos dados pessoais, a autoridade nacional competente, atendendo aos efeitos adversos prováveis da violação, pode exigir essa notificação.
A notificação ao assinante ou ao indivíduo indica, pelo menos, a natureza da violação de dados pessoais e os pontos de contacto onde podem ser obtidas informações complementares e recomendará medidas destinadas a limitar eventuais efeitos adversos da violação dos dados pessoais. A notificação à autoridade nacional competente indica ainda as consequências da violação de dados pessoais e as medidas propostas ou tomadas pelo prestador para fazer face a essa violação.

4. As autoridades nacionais competentes podem adotar orientações, sujeitas às medidas técnicas de execução aprovadas nos termos do n.º 5 e, se for caso disso, emitir instruções sobre as circunstâncias em que os prestadores estão obrigados a comunicar violações de dados pessoais e a forma e processo aplicáveis a essa notificação.
As referidas autoridades devem igualmente ter a possibilidade de verificar se os prestadores cumpriram as suas obrigações de notificação nos termos do presente número e aplicar sanções adequadas em caso de não cumprimento.
Os prestadores devem manter um registo das violações de dados pessoais, com a indicação dos factos que lhes dizem respeito, dos seus efeitos e das medidas de reparação tomadas, registo que deve ser suficiente para que as autoridades nacionais competentes possam verificar o cumprimento do disposto no n.º 3. O registo inclui apenas a informação necessária para esse efeito.

5. Para assegurar coerência na aplicação das medidas a que se referem os n.os 2, 3 e 4, a Comissão poderá, após consulta da Agência Europeia para a Segurança das Redes e da Informação (ENISA), do Grupo de Proteção

das Pessoas no que respeita ao Tratamento de Dados Pessoais instituído nos termos do artigo 29.º da Diretiva 95/46/CE, e da Autoridade Europeia para a Proteção de Dados, aprovar medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação a que se refere o presente artigo. Na aprovação dessas medidas, a Comissão deve envolver todos os interessados, de modo, designadamente, a ser informada sobre os melhores meios técnicos e económicos disponíveis para a aplicação do presente artigo.
Essas medidas, que têm por objeto alterar elementos não essenciais da presente diretiva, são aprovadas pelo procedimento de regulamentação com controlo a que se refere o n.º 2 do artigo 14.º-A.

Artigo 5.º Confidencialidade das comunicações
1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.

2. O n.º 1 não se aplica às gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas para o efeito de constituir prova de uma transação comercial ou de outra comunicação de negócios.

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de

uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.

Artigo 6.º Dados de tráfego

1. Sem prejuízo do disposto nos n.os 2, 3 e 5 do presente artigo e no n.º 1 do artigo 15.º, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2. Podem ser tratados dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações. O referido tratamento é lícito apenas até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.

3. Para efeitos de comercialização dos serviços de comunicações eletrónicas ou para a prestação de serviços de valor acrescentado, o prestador de um serviço de comunicações eletrónicas acessível ao público pode tratar os dados referidos no n.º 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou essa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento prévio. Deve ser dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego.

4. O prestador de serviços informará o assinante ou utilizador dos tipos de dados de tráfego que são tratados e da duração desse tratamento para os fins mencionados no n.º 2 e, antes de obtido o consentimento, para os fins mencionados no n.º 3.

5. O tratamento de dados de tráfego, em conformidade com o disposto nos n.os 1 a 4, será limitado ao pessoal que trabalha para os fornecedores de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis encarregado da faturação ou da gestão do tráfego, das informações a clientes, da deteção de fraudes, da comercialização dos serviços de comunicações eletrónicas publicamente

disponíveis, ou da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas atividades.
6. Os n.os 1, 2, 3 e 5 são aplicáveis sem prejuízo da possibilidade de os organismos competentes serem informados dos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial os litígios relativos a interligações ou à faturação.

Artigo 7.º Faturação detalhada
1. Os assinantes têm o direito de receber faturas não detalhadas.

2. Os Estados-Membros aplicarão disposições nacionais para conciliar os direitos dos assinantes que recebem faturas detalhadas com o direito à privacidade dos utilizadores autores das chamadas e dos assinantes chamados, garantindo, por exemplo, que se encontrem à disposição desses utilizadores e assinantes meios alternativos suficientes para comunicações ou pagamentos que protejam melhor a privacidade.

Artigo 8.º Apresentação e restrição da identificação da linha chamadora e da linha conectada
1. Quando for oferecida a apresentação da identificação da linha chamadora, o prestador de serviços deve dar ao utilizador que efetua a chamada a possibilidade de impedir, chamada a chamada e através de um meio simples e gratuito, a apresentação da identificação da linha chamadora. Esta possibilidade deve ser oferecida, linha a linha, aos assinantes que efetuam chamadas.

2. Quando for oferecida a apresentação da identificação da linha chamadora, o prestador de serviços deve dar ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito no caso de uma utilização razoável desta função, a apresentação da identificação da linha chamadora nas chamadas de entrada.

3. Quando for oferecida a apresentação da identificação da linha chamadora, caso a identificação dessa linha seja apresentada antes do estabelecimento da chamada, o prestador de serviços deve dar ao assinante chamado a possibilidade de rejeitar, através de um meio simples, chamadas de entrada quando a apresentação da identificação da linha chamadora tiver sido impedida pelo utilizador ou assinante que efetua a chamada.

4. Quando for oferecida a apresentação da identificação da linha conectada, o prestador de serviços deve dar ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito, a apresentação da identificação da linha conectada ao utilizador que efectua a chamada.

5. O n.º 1 é igualmente aplicável às chamadas para países terceiros originadas na Comunidade. Os n.os 2, 3 e 4 são igualmente aplicáveis a chamadas de entrada originadas em países terceiros.

6. Os Estados-Membros garantirão que, quando for oferecida a apresentação da identificação da linha chamadora e/ou da linha conectada, os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis informarão o público do facto e das possibilidades referidas nos n.os 1 a 4.

Artigo 9.º Dados de localização para além dos dados de tráfego

1. Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. Os utilizadores ou assinantes devem dispor da possibilidade de retirar em qualquer momento o seu consentimento para o tratamento dos dados de localização, para além dos dados de tráfego.

2. Nos casos em que tenha sido obtido o consentimento dos utilizadores ou assinantes para o tratamento de dados de localização para além dos dados de tráfego, o utilizador ou assinante deve continuar a ter a possibilidade de, por meios simples e gratuitos, recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação.

3. O tratamento de dados de localização para além dos dados de tráfego, em conformidade com os n.os 1 e 2, deve ficar reservado ao pessoal que trabalha

para o fornecedor de redes públicas de comunicações ou de serviços de comunicações eletrónicas publicamente disponíveis ou para terceiros que forneçam o serviço de valor acrescentado, devendo restringir-se ao necessário para efeitos de prestação do serviço de valor acrescentado.

Artigo 10.º Exceções
Os Estados-Membros velarão pela transparência dos processos que regem o modo como os fornecedores de uma rede de comunicações públicas e/ou de um serviço de comunicações eletrónicas publicamente disponível podem dispensar:
a) A eliminação da apresentação da identificação da linha chamadora, temporariamente e a pedido de um assinante que pretenda determinar a origem de chamadas mal intencionadas ou incomodativas; nestes casos, em conformidade com a legislação nacional, os dados que contêm a identificação do assinante que efetua a chamada serão armazenados e disponibilizados pelo fornecedor da rede de comunicações públicas e/ou serviço de comunicações eletrónicas publicamente disponível;

b) A eliminação da apresentação da identificação da linha chamadora e a recusa temporária ou ausência de consentimento de um assinante ou utilizador para o tratamento de dados de localização, linha a linha, para as organizações que recebem chamadas de emergência e são reconhecidas como tal pelos Estados-Membros, incluindo as autoridades encarregadas de aplicar a lei e os serviços de ambulâncias e de bombeiros, para efeitos de resposta a essas chamadas.

Artigo 11.º Reencaminhamento automático de chamadas
Os Estados-Membros assegurarão que qualquer assinante possa, gratuitamente e através de um meio simples, pôr fim ao reencaminhamento automático de chamadas por terceiros para o seu equipamento terminal.

Artigo 12.º Listas de assinantes
1. Os Estados-Membros assegurarão que os assinantes sejam informados, gratuitamente e antes de serem incluídos nas listas, dos fins a que se destinam as listas de assinantes impressas ou eletrónicas publicamente disponíveis ou que podem ser obtidas através de serviços de informações de listas, nas quais os seus dados pessoais podem ser incluídos, bem como de quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões eletrónicas da lista.

2. Os Estados-Membros assegurarão que os assinantes disponham da possibilidade de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, de quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, como estipulado pelo fornecedor das listas, bem como de verificar, corrigir ou retirar esses dados. A não inclusão numa lista pública de assinantes, a verificação, a correção e a retirada de dados pessoais da mesma devem ser gratuitas.

3. Os Estados-Membros poderão exigir que o consentimento adicional dos assinantes seja solicitado para qualquer utilização de uma lista pública que não a busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação.

4. Os n.^{os} 1 e 2 aplicam-se aos assinantes que sejam pessoas singulares. Os Estados-Membros assegurarão igualmente, no âmbito do direito comunitário e das legislações nacionais aplicáveis, que os interesses legítimos dos assinantes que não sejam pessoas singulares sejam suficientemente protegidos no que se refere à sua inclusão em listas públicas.

Artigo 13.º Comunicações não solicitadas

1. A utilização de sistemas de chamada e de comunicação automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio eletrónico para fins de comercialização direta apenas pode ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio.

2. Não obstante o n.º 1, se uma pessoa singular ou coletiva obtiver dos seus clientes as respetivas coordenadas eletrónicas de contacto para correio eletrónico, no contexto da venda de um produto ou serviço, nos termos da Diretiva 95/46/CE, essa pessoa singular ou coletiva pode usar essas coordenadas eletrónicas de contacto para fins de comercialização direta dos seus próprios produtos ou serviços análogos, desde que aos clientes tenha sido dada clara e distintamente a possibilidade de recusarem, de forma gratuita e fácil, a utilização dessas coordenadas eletrónicas de contacto no momento da respetiva recolha e por ocasião de cada mensagem, quando o cliente não tenha inicialmente recusado essa utilização.

3. Os Estados-Membros tomam as medidas adequadas para assegurar que as comunicações não solicitadas para fins de comercialização direta em casos diferentes dos referidos nos n.os 1 e 2 não sejam permitidas quer sem o consentimento dos assinantes ou utilizadores em questão, quer em relação a assinantes ou utilizadores que não desejam receber essas comunicações, sendo a escolha entre estas opções determinada pela legislação nacional, tendo em conta que ambas as opções devem ser gratuitas para o assinante ou utilizador.

4. Em todo o caso, é proibida a prática do envio de correio eletrónico para fins de comercialização direta, dissimulando ou escondendo a identidade da pessoa em nome da qual é efetuada a comunicação, em violação do artigo 6.º da Diretiva 2000/31/CE, sem um endereço válido para o qual o destinatário possa enviar um pedido para pôr termo a essas comunicações ou que incentive os destinatários a visitar sítios internet que violem o disposto no referido artigo.

5. O disposto nos n.os 1 e 3 aplica-se aos assinantes que sejam pessoas singulares. Os Estados-Membros asseguram igualmente, no âmbito do direito comunitário e das legislações nacionais aplicáveis, que os interesses legítimos dos assinantes que não sejam pessoas singulares sejam suficientemente protegidos no que se refere a comunicações não solicitadas.

6. Sem prejuízo de eventuais recursos administrativos que venham a ser previstos, nomeadamente ao abrigo do n.º 2 do artigo 15.º-A, os Estados-Membros asseguram que as pessoas singulares ou coletivas prejudicadas por infrações às disposições nacionais aprovadas nos termos do presente artigo e que tenham um interesse legítimo na cessação ou proibição dessas infrações, nomeadamente um prestador de serviços de comunicações eletrónicas que proteja os seus interesses comerciais legítimos, possam intentar ações judiciais contra tais infrações. Os Estados-Membros podem ainda estabelecer regras específicas sobre as sanções aplicáveis a prestadores de serviços de comunicações eletrónicas que pela sua negligência contribuam para infrações às disposições nacionais aprovadas nos termos do presente artigo.

Artigo 14.º Características técnicas e normalização

1. Na execução do disposto na presente diretiva, os Estados-Membros garantirão, sem prejuízo do disposto nos n.os 2 e 3, que não sejam impostos requisitos obrigatórios sobre características técnicas específicas

dos equipamentos terminais ou de outros equipamentos de comunicações eletrónicas que possam impedir a colocação no mercado e a livre circulação desses equipamentos nos Estados-Membros e entre estes.

2. Nos casos em que a execução das disposições da presente diretiva só possa ser feita através da exigência de características técnicas específicas em redes de comunicações eletrónicas, os Estados-Membros informarão a Comissão nos termos do procedimento previsto na Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de Junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação[65].

3. Caso seja necessário, poderão ser adotadas medidas para garantir que o equipamento terminal seja construído de uma forma compatível com o direito de os utilizadores protegerem e controlarem a utilização dos seus dados pessoais, em conformidade com o disposto na Diretiva 1999/5/CE e na Decisão 87/95/CEE do Conselho, de 22 de Dezembro de 1986, relativa à normalização no domínio das tecnologias da informação e das telecomunicações[66].

Artigo 14.º-A Procedimento de comité

1. A Comissão é assistida pelo Comité das Comunicações, criado pelo artigo 22.º da Diretiva 2002/21/CE (Diretiva-Quadro).

2. Sempre que se faça referência ao presente número, são aplicáveis os n.os 1 a 4 do artigo 5.º-A e o artigo 7.º da Decisão 1999/468/CE, tendo-se em conta o disposto no seu artigo 8.º.

3. Sempre que se faça referência ao presente número, são aplicáveis os n.os 1, 2, 4 e 6 do artigo 5.º-A e o artigo 7.º da Decisão 1999/468/CE, tendo-se em conta o disposto no seu artigo 8.º.

Artigo 15.º Aplicação de determinadas disposições da Diretiva 95/46/CE

1. Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas

[65] JO L 204 de 21.7.1998, p. 37. Diretiva alterada pela Diretiva 98/48/CE (JO L 217 de 5.8.1998, p. 18).

[66] JO L 36 de 7.2.1987, p. 31. Decisão com a última redação que lhe foi dada pelo Ato de Adesão de 1994.

restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.

1-A. O n.º 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações[67], para os fins mencionados no n.º 1 do artigo 1.º dessa diretiva.

1.-B. Os prestadores estabelecem procedimentos internos para responder aos pedidos de acesso aos dados pessoais dos utilizadores com base nas disposições nacionais aprovadas nos termos do n.º 1. Aqueles prestam às autoridades nacionais competentes, a pedido destas, informação sobre esses procedimentos, o número de pedidos recebidos, a justificação jurídica invocada e a resposta dada.

2. O disposto no capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções é aplicável no que respeita às disposições nacionais adotadas nos termos da presente diretiva e aos direitos individuais decorrentes da presente diretiva.

3. O Grupo de Proteção das Pessoas no que respeita ao Tratamento de Dados Pessoais, instituído nos termos do artigo 29.º da Diretiva 95/46/CE, realizará também as tarefas previstas no artigo 30.º da mesma diretiva no que respeita às matérias abrangidas pela presente diretiva, nomeadamente a proteção dos direitos e liberdades fundamentais e dos interesses legítimos no sector das comunicações eletrónicas.

---

[67] JO L 105 de 13.4.2006, p. 54.

Artigo 15.º-A Aplicação e execução

1. Os Estados-Membros estabelecem as regras relativas às sanções, incluindo, se for esse o caso, as de natureza penal, aplicáveis às infrações de disposições nacionais aprovadas por força da presente diretiva e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser eficazes, proporcionadas e dissuasivas e podem ser aplicadas para abranger a duração de qualquer infração, mesmo que tenha posteriormente cessado. Os Estados-Membros notificam essas disposições à Comissão até 25 de Maio de 2011, devendo notificá-la imediatamente de quaisquer alterações subsequentes das mesmas.

2. Sem prejuízo de qualquer solução judicial eventualmente disponível, os Estados-Membros asseguram que a autoridade nacional competente e, se for caso disso, outros organismos nacionais disponham de poderes para ordenar a cessação das infrações a que se refere o n.º 1.

3. Os Estados-Membros asseguram que as autoridades nacionais competentes e, se for caso disso, outros organismos nacionais, disponham dos poderes e recursos de investigação necessários, nomeadamente o poder de obterem quaisquer informações relevantes de que necessitem para acompanhar e fazer cumprir as disposições nacionais aprovadas nos termos da presente diretiva.

4. As autoridades reguladoras nacionais competentes podem aprovar medidas para assegurar uma cooperação transfronteiriça eficaz na execução da legislação nacional aprovada nos termos da presente diretiva e para criar condições harmonizadas na oferta de serviços que envolvem fluxos transfronteiriços de dados.
As autoridades reguladoras nacionais apresentam à Comissão, em tempo útil antes da aprovação dessas medidas, um resumo dos motivos para a ação, os requisitos previstos e as ações propostas. A Comissão pode, depois de ter examinado essas informações e após consulta da ENISA e do Grupo de Proteção das Pessoas no que respeita ao Tratamento de Dados Pessoais criado nos termos do artigo 29.º da Diretiva 95/46/CE, formular observações ou recomendações sobre aquelas, em especial para garantir que os requisitos não afetam negativamente o bom funcionamento do mercado interno. As autoridades reguladoras nacionais têm o mais possível em conta as observações ou recomendações da Comissão ao decidir sobre as medidas.

Artigo 16.º Disposições transitórias

1. O disposto no artigo 12.º não é aplicável às edições de listas já elaboradas ou colocadas no mercado, em formato impresso ou eletrónico off-line, antes da entrada em vigor das disposições nacionais adotadas nos termos da presente diretiva.

2. No caso de os dados pessoais dos assinantes de serviços públicos fixos ou móveis de telefonia vocal terem sido incluídos numa lista pública de assinantes, em conformidade com o disposto na Diretiva 95/46/CE (e no artigo 11.º da Diretiva 97/66/CE, antes da entrada em vigor das disposições nacionais adotadas nos termos da presente diretiva, os dados pessoais desses assinantes podem manter-se nessa lista pública nas suas versões impressa ou eletrónica, incluindo versões com funções de pesquisa inversa, a menos que os assinantes se pronunciem em contrário depois de terem recebido informação completa sobre as finalidades e as opções, em conformidade com o disposto no artigo 12.º da presente diretiva.

Artigo 17.º Transposição

1. Antes de 31 de Outubro de 2003, os Estados-Membros devem pôr em vigor as disposições necessárias para dar cumprimento à presente diretiva e informar imediatamente a Comissão desse facto.
Quando os Estados-Membros aprovarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da publicação oficial. As modalidades de referência são aprovadas pelos Estados-Membros.

2. Os Estados-Membros devem comunicar à Comissão as disposições de direito interno que aprovarem nas matérias reguladas pela presente diretiva, bem como quaisquer alterações a essas disposições.

Artigo 18.º Cláusula de revisão

A Comissão apresentará ao Parlamento Europeu e ao Conselho, no prazo de três anos a contar da data referida no n.º 1 do artigo 17.º, um relatório sobre a sua aplicação e os respetivos efeitos nos operadores económicos e nos consumidores, nomeadamente no respeitante às disposições relativas a comunicações não solicitadas, e tendo em consideração o ambiente internacional. Para tal, a Comissão pode solicitar informações aos Estados-Membros, as quais devem ser fornecidas sem atraso indevido. Caso se revele apropriado, a Comissão apresentará propostas de alteração

da presente diretiva com o objetivo de ter em consideração os resultados do relatório atrás mencionado e quaisquer mudanças observadas no sector, bem como toda e qualquer outra proposta considerada necessária para reforçar a eficácia da presente diretiva.

Artigo 19.º Revogação
A Diretiva 97/66/CE é revogada a partir da data referida no n.º 1 do artigo 17.º As remissões para a diretiva revogada devem entender-se como sendo feitas para a presente diretiva.

Artigo 20.º Entrada em vigor
A presente diretiva entra em vigor no dia da sua publicação no Jornal Oficial das Comunidades Europeias.

Artigo 21.º Destinatários
Os Estados-Membros são os destinatários da presente diretiva.

Feito em Bruxelas,

em 12 de Julho de 2002.

Pelo Parlamento Europeu

O Presidente

P. COX

Pelo Conselho
O Presidente
T. PEDERSEN

15. Decreto-Lei nº 58/2000, de 18 de Abril, transpõe para o direito interno a Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de julho, relativa aos procedimentos de informação no domínio das normas e regulamentações técnicas e às regras relativas aos serviços da sociedade da informação

Os serviços da sociedade da informação, em que se incluem as regras específicas dos serviços prestados a distância, necessitam de uma especial atenção naquilo que diz respeito à sua regulamentação.

Esta matéria, bem como a que diz respeito às normas e regulamentações técnicas, tem contornos específicos que se prendem com a globalização dos mercados. Esta implica a necessidade de eliminar ou, pelo menos, reduzir os obstáculos ao comércio de produtos industriais e agrícolas, incluindo os provenientes da pesca, bem como a necessidade de assegurar a livre prestação de serviços no domínio da sociedade da informação no âmbito do território comunitário.

Urge, pois, transpor para a ordem jurídica interna a Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho, que altera a Diretiva n.º 98/34/CE, do Parlamento Europeu e do Conselho, de 22 de Junho, a qual se designa «diretiva do Parlamento Europeu e do Conselho relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação».

A Diretiva n.º 98/34/CE é codificadora de anteriores, como é o caso da Diretiva n.º 83/189/CEE, do Conselho, de 28 de Março.

Esta última diretiva estabeleceu um procedimento de notificação prévia, no domínio das normas e das regulamentações técnicas, com a finalidade de permitir uma maior transparência das iniciativas nacionais e a livre circulação de mercadorias e de garantir o bom funcionamento do mercado interno. Posteriormente, foi alterada pela Diretiva n.º 88/182/CEE, do Conselho, de 22 de Março, e pela Diretiva n.º 94/10/CE, do Parlamento Europeu e do Conselho, de 23 de Março, e transposta para o direito interno pelas Resoluções do Conselho de Ministros n.^{os} 41/90, de 13 de Outubro, e 95/95, de 3 de Outubro.

Foi, contudo, a diretiva que agora se transpõe para a ordem jurídica interna, Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho, que veio modificar a Diretiva n.º 98/34/CE, ampliando o seu campo de aplicação.

Prevê-se no presente diploma que o organismo português responsável pelas atividades de normalização - Instituto Português da Qualidade - fique obrigado a proceder à notificação da Comissão Europeia e dos organismos europeus de normalização dos demais Estados membros das regras específicas que se prendem com normas técnicas e com os serviços prestados a distância e por via eletrónica, relativamente aos serviços da sociedade da informação. Ficam também abrangidas por esse procedimento as regras que dizem respeito ao acesso ao exercício daquela atividade, como é o caso das relativas ao estabelecimento dos prestadores desses serviços, em especial as que se prendem com o regime de autorização e de licença, mesmo que essas regras estejam incluídas em regulamentação com um objetivo mais geral.
Todos os outros serviços e organismos da Administração Pública com competências nessas matérias devem, através daquele organismo, canalizar todos os assuntos sujeitos a notificação, sendo através dele também canalizada toda a informação fornecida pela Comissão Europeia.
Excluem-se do âmbito do presente diploma as licenças em matéria de telecomunicações, certas disposições relativas ao exercício de atividades de radiodifusão televisiva, bem como os casos excecionais em que situações graves e imprevisíveis obriguem a medidas urgentes.
Assim:
Nos termos da alínea a) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

Artigo 1.º Objetivo e âmbito de aplicação
O presente diploma estabelece os procedimentos administrativos a que obedece a troca de informação no domínio das normas e das regulamentações técnicas, bem como das regras, relativas aos serviços da sociedade da informação, transpondo para a ordem jurídica interna a Diretiva n.º 98/34/CE, do Parlamento Europeu e do Conselho, de 22 de Junho, alterada pela Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho.

Artigo 2.º Definições
Para efeitos de aplicação do presente diploma, entende-se por:
a) «Produto» qualquer bem de fabrico industrial ou agrícola, incluindo os provenientes da pesca;

b) «Serviço» qualquer prestação de atividade a distância, por via eletrónica e mediante pedido individual do seu destinatário, geralmente mediante

remuneração, considerando-se, para efeitos da presente definição:
i) «A distância» um serviço prestado sem que as partes estejam simultaneamente presentes;

ii) «Por via eletrónica» um serviço enviado da origem e recebido no destino através de meios eletrónicos de processamento e de armazenamento de dados que seja inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos;

iii) «Mediante pedido individual do seu destinatário» um serviço fornecido por transmissão de dados mediante um pedido individualizado;

c) «Especificação técnica» a discriminação que consta de um documento em que se definam:
i) As características exigidas a um produto, tais como os níveis de qualidade, a propriedade de utilização, a segurança, as dimensões, incluindo as prescrições que lhe são aplicáveis no que respeita à denominação de venda, à terminologia, aos símbolos, aos ensaios e respetivos métodos, à embalagem, à marcação e rotulagem, bem como aos procedimentos de avaliação da conformidade;

ii) Os métodos e os processos de produção relativos aos produtos agrícolas, ao abrigo do n.º 1 do artigo 32.º do Tratado que instituiu as Comunidades Europeias;

iii) Os métodos e os processos de produção relativos aos produtos destinados à alimentação humana e animal;

iv) Os métodos e os processos relativos aos medicamentos definidos no artigo 3.º do Decreto-Lei n.º 72/91, de 8 de Fevereiro;

v) Os métodos e os processos de produção relativos a outros produtos que revistam as mesmas características dos referidos na alínea anterior;

d) «Outra exigência» qualquer requisito que, não constituindo uma especificação técnica, seja imposto a um produto, por motivos de defesa, nomeadamente dos consumidores ou do ambiente, e que vise o seu ciclo de vida após colocação no mercado, em que se incluem as condições da respetiva utilização, de reciclagem, de reutilização ou de eliminação,

sempre que essas condições possam influenciar significativamente a composição ou a natureza do produto ou a sua comercialização;

e) «Norma» a especificação técnica aprovada por um organismo reconhecido que exerça atividade de normalização para aplicação repetida ou contínua, cujo cumprimento não é obrigatório, e que pertença a uma das seguintes categorias:
i) Norma internacional - norma adotada por uma organização internacional de normalização e colocada à disposição do público;

ii) Norma europeia - norma adotada por um organismo europeu de normalização e colocada à disposição do público;

iii) Norma nacional - norma adotada por um organismo nacional de normalização e colocada à disposição do público;

f) «Projeto de norma» o documento com o texto das especificações técnicas que se prevê venham a ser adotadas relativamente a um assunto determinado, de acordo com os procedimentos de normalização nacional, tal como resulta dos trabalhos preparatórios difundidos para comentário ou inquérito público;

g) «Regra técnica» a especificação técnica ou outro requisito, regra ou exigência relativa aos serviços, incluindo as disposições regulamentares internas que lhes são aplicáveis e cujo cumprimento seja obrigatório, de jure ou de facto, para a comercialização, a utilização, a prestação de serviços ou o estabelecimento de um operador de serviços, abrangendo, nomeadamente:
i) As disposições legais e regulamentares que remetam para especificações técnicas, outros requisitos ou regras relativas aos serviços ou para códigos profissionais ou de boa prática;

ii) Os acordos voluntários em que uma entidade pública seja parte contratante e que visem, numa perspetiva de interesse geral, a observância de especificações técnicas, de outros requisitos ou de regras relativas aos serviços, com exceção dos cadernos de encargos dos contratos públicos;

iii) As especificações técnicas, outros requisitos ou regras relativas aos serviços relacionados com medidas de carácter fiscal ou financeiro que

afetem o consumo dos produtos ou dos serviços e que se destinem a garantir a observância das referidas especificações técnicas, outros requisitos ou regras relativas aos serviços, com exceção dos relacionados com os regimes nacionais de segurança social;

h) «Projeto de regra técnica» o texto de uma especificação técnica, de outro requisito ou de uma regra relativa aos serviços, incluindo disposições regulamentares internas, elaborado com o objetivo de ser adotado como regra técnica e que se encontre numa fase de preparação que permita ainda a introdução de alterações substanciais;
i) «Regra relativa aos serviços» qualquer requisito de natureza geral especificamente relacionado com o acesso às atividades incluídas nos serviços referidos na alínea b) do presente artigo, com o seu exercício, bem como com qualquer disposição relativa ao próprio serviço ou relativa aos respetivos prestadores e destinatários, considerando-se que:
i) Uma regra tem em vista especificamente os serviços da sociedade da informação sempre que a sua motivação e o texto do seu articulado tenham como objetivo específico, na totalidade ou em algumas disposições, regulamentar de modo explícito e circunscrito esses serviços;

ii) Uma regra não tem em vista os serviços da sociedade da informação caso diga apenas respeito a esses serviços de modo implícito ou incidental.

Artigo 3.º Organismo competente para a notificação
Compete ao Instituto Português da Qualidade, adiante designado «organismo de notificação», gerir a informação relativa às normas e regras técnicas a que se refere o presente diploma.

Artigo 4.º Atribuições dos organismos regulamentadores
1. Os serviços que pretendam elaborar regras técnicas relativas aos produtos ou regras relativas aos serviços definidos no artigo 2.º do presente diploma devem, através do organismo de notificação:
a) Comunicar, de imediato, à Comissão Europeia qualquer projeto de regra técnica;

b) Transmitir, simultaneamente, o texto das disposições legislativas e regulamentares de base, caso o seu conhecimento seja necessário para apreciar o alcance do projeto de regra técnica, salvo se já tiver sido apresentado com uma comunicação anterior;

c) Comunicar, nas condições referidas na alínea anterior, as alterações significativas ao projeto de regras técnicas que tenham por efeito modificar o âmbito de aplicação, reduzir o calendário de aplicação inicialmente previsto ou aditar especificações e outras exigências, tornando-as mais rigorosas;

d) Comunicar, se for o caso, um resumo ou as referências dos dados pertinentes de um projeto de regra técnica que se destine, em especial, a limitar a comercialização ou a utilização de uma substância, de uma preparação ou de um produto químico, designadamente por razões de saúde pública, defesa dos consumidores ou proteção do ambiente;

e) Comunicar também, se for o caso, um resumo ou as referências dos dados pertinentes relativos à substância, à preparação ou ao produto em causa e os referentes aos produtos alternativos conhecidos e disponíveis à medida que tais informações se tornem acessíveis, bem como os efeitos previsíveis da medida sobre a saúde pública, a defesa dos consumidores e a proteção do ambiente, efetuando, quando necessário, uma análise de risco, de acordo com os princípios gerais de avaliação de riscos dos produtos químicos referidos no n.º 4 do artigo 10.º do Regulamento (CEE) n.º 793/93, do Conselho, de 23 de Março, quando se trate de uma substância existente a que alude o artigo 7.º do Decreto-Lei n.º 82/95, de 22 de Abril, ou quando se trate de uma nova substância;

f) Comunicar, de imediato, à Comissão Europeia o texto definitivo de qualquer regra técnica, sem prejuízo do disposto no n.º 2 do artigo 6.º;

g) Ponderar na elaboração final de uma regra técnica as observações que tenham sido feitas pela Comissão ou por outros Estados membros sobre o respetivo projeto.

2. Os serviços interessados podem, através do organismo de notificação, dirigir a qualquer Estado membro que tenha apresentado um projeto de regra técnica as observações e os comentários que se afigurem pertinentes relativamente a matéria que seja suscetível de entravar as trocas comerciais.

3. Pode ser requerida, expressamente, a confidencialidade da notificação através de pedido devidamente fundamentado, sem prejuízo de ser permitido aos serviços da Administração Pública, adotando as precauções

necessárias, efetuarem consultas, para efeitos de peritagem, através de pessoas singulares ou coletivas.

Artigo 5.º Prazos de aprovação dos projetos de regras técnicas
1. Nenhum projeto de regra técnica pode ser aprovado antes do decurso de três meses contados a partir da data da sua receção pela Comissão.

2. O prazo referido no número anterior passa a ser de 4, 6, 12 ou 18 meses, nas condições referidas nas alíneas seguintes:
a) 4 meses:
i) Quando o projeto de regra técnica adotar a forma de acordo voluntário em que uma entidade pública seja parte contratante e que vise, numa perspetiva de interesse geral, a observância de especificações técnicas ou de outras exigências, com exceção dos cadernos de encargos dos contratos públicos;

ii) Quando se tratar de um projeto de regra a adotar relativo aos serviços definidos no artigo 2.º;

b) 6 meses, quando se tratar da adoção de projeto de regra técnica não relativa aos serviços, se, no prazo de 3 meses a contar da sua receção pela Comissão, esta ou outro Estado membro emitir parecer circunstanciado no sentido de a medida prevista conter aspetos eventualmente contrários à livre circulação de mercadorias;

c) 12 meses:
i) Quando se tratar da adoção de projeto de regras técnicas, com exclusão das relativas aos serviços, a contar da data da receção pela Comissão, se, no prazo de 3 meses, esta manifestar intenção de propor ou adotar uma diretiva, um regulamento ou uma decisão sobre a matéria, nos termos do artigo 249.º do Tratado que instituiu as Comunidades Europeias;

ii) Quando a Comissão, nos 3 meses subsequentes à data da sua receção, verificar que o projeto de regra técnica incide sobre matéria abrangida por uma proposta de diretiva, de regulamento ou de decisão apresentada ao Conselho nos termos do artigo 249.º do Tratado que instituiu as Comunidades Europeias;
d) 18 meses, se o Conselho adotar uma posição comum durante o período referido na alínea anterior, sem prejuízo do disposto no n.º 4 do presente artigo.

3. O prazo a que se refere a alínea a) do número anterior conta-se a partir da data da receção pela Comissão do projeto se, nos três meses subsequentes, esta instituição ou outro Estado membro emitir um parecer circunstanciado segundo o qual a medida prevista poderá, eventualmente, criar obstáculos à livre circulação dos serviços ou à sua liberdade de estabelecimento.

4. As obrigações a que se referem as alíneas b) e c) do n.º 2 cessam quando a Comissão informar os Estados membros que renuncia a propor ou a adotar um ato comunitário vinculativo ou que retira o seu projeto ou proposta e ainda quando o Conselho adotar, nesse domínio, um ato comunitário vinculativo.

Artigo 6.º Exceções

1. O disposto nos artigos 4.º e 5.º deste diploma não é aplicável às disposições legislativas e regulamentares ou aos acordos voluntários que, em matéria de especificações técnicas, prossigam as seguintes finalidades:
a) Dar cumprimento a atos comunitários vinculativos cujo efeito seja a adoção de especificações técnicas ou de regras relativas aos serviços;

b) Observar os compromissos decorrentes de um acordo internacional cujo efeito seja a adoção de especificações técnicas ou de regras relativas aos serviços e que sejam comuns a toda a Comunidade;

c) Invocar cláusulas de salvaguarda previstas em atos comunitários vinculativos;

d) Aplicar o regime previsto no Decreto-Lei n.º 311/95, de 20 de Novembro, relativo à segurança geral dos produtos;

e) Dar apenas execução a acórdão do Tribunal de Justiça das Comunidades Europeias;

f) Alterar apenas uma regra técnica na aceção da alínea g) do artigo 2.º do presente diploma, de acordo com um pedido da Comissão, tendo em vista eliminar entraves às trocas comerciais.

2. Não é igualmente aplicável o disposto no artigo 4.º quando se trate de mera transposição integral de uma norma internacional ou europeia, bastando, neste caso, disponibilizar a adequada informação à Comissão sobre essa norma.
3. A informação referida no número anterior deve ser acompanhada de notificação da qual conste a sua justificação, salvo se esta se depreender, claramente, do projeto.

4. O disposto nas alíneas b) e c) do n.º 2 do artigo 5.º não se aplica aos acordos voluntários a que se refere o ponto ii) da alínea g) do artigo 2.º

5. O disposto no artigo 5.º do presente diploma também não é aplicável:
a) Às disposições legislativas e regulamentares que visem a proibição de fabrico, na medida em que não entravem a livre circulação de produtos;

b) Às especificações técnicas ou outros requisitos, bem como às regras, relativos aos serviços a que se refere a alínea b) do artigo 2.º deste diploma.

Artigo 7.º Procedimento de urgência
1. O disposto no artigo 5.º não é aplicável quando, por razões de urgência resultantes de uma situação grave e imprevisível, que envolva a defesa da saúde das pessoas e dos animais, a preservação das plantas, a segurança e a ordem públicas, nomeadamente a proteção dos menores, seja necessário elaborar, com a maior brevidade, regras técnicas, a adotar e a aplicar de imediato.

2. Não é também aplicável o disposto no artigo 5.º deste diploma quando, por razões de urgência resultantes de uma situação grave que envolva a proteção da segurança e integridade do sistema financeiro, nomeadamente a defesa dos depositantes, investidores ou segurados, se torne necessário adotar e aplicar de imediato regras relativas a serviços financeiros.

3. Na comunicação referida na alínea a) do n.º 1 do artigo 4.º devem constar os motivos que justificam a urgência das medidas em questão.

Artigo 8.º Serviços não abrangidos
Os serviços não abrangidos pelo presente diploma são os indicados no anexo I do presente diploma, que dele faz parte integrante.

Artigo 9.º Referência às diretivas
A adoção de regras técnicas pela legislação nacional deve fazer referência à Diretiva n.º 98/34/CE, do Parlamento Europeu e do Conselho, de 22 de Junho, com as alterações introduzidas pela Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho.

Artigo 10.º Norma revogatória
É revogada a Resolução do Conselho de Ministros n.º 95/95, de 3 de Outubro.

Artigo 11.º Entrada em vigor
O presente diploma entra em vigor no dia seguinte ao da sua publicação.
Visto e aprovado em Conselho de Ministros de 2 de Março de 2000.
Jaime José Matos da Gama
Joaquim Augusto Nunes Pina Moura.
Joaquim Augusto Nunes Pina Moura.
Promulgado em 31 de Março de 2000.
Publique-se.
O Presidente da República,
JORGE SAMPAIO.
Referendado em 6 de Abril de 2000.
O Primeiro-Ministro,
António Manuel de Oliveira Guterres.

ANEXO I

(REFERIDO NO ARTIGO 8.º)
LISTA DOS SERVIÇOS QUE NÃO ESTÃO ABRANGIDOS PELO PRESENTE DIPLOMA

1. O presente diploma não é aplicável:
a) Aos serviços de radiodifusão sonora;

b) Aos serviços de radiodifusão televisiva referidos na alínea a) do artigo 1.º da Diretiva n.º 89/552/CEE, do Conselho, de 3 de Outubro;

c) Às regras relativas a questões sujeitas à regulamentação comunitária em matéria de serviços de telecomunicações definidos na Diretiva n.º 90/387/CEE, do Conselho, de 28 de Junho;

d) Às regras relativas a questões sujeitas à regulamentação comunitária em matéria de serviços financeiros;

e) Às regras enunciadas pelos ou para os mercados regulamentados na aceção da Diretiva n.º 93/22/CE, do Conselho, de 10 de Maio, outros mercados ou órgãos que efetuam operações de compensação ou de liquidação desses mercados, sem prejuízo do disposto na alínea f) do artigo 4.º do presente diploma.

2. O presente diploma também não é aplicável aos serviços prestados na presença física do prestador e do destinatário, ainda que a sua prestação implique a utilização de dispositivos eletrónicos:

a) Exames ou tratamentos num consultório médico por meio de equipamentos eletrónicos, mas na presença física do paciente;

b) Consulta de um catálogo eletrónico num estabelecimento comercial na presença física do cliente;

c) Reserva de um bilhete de avião através de uma rede de computadores numa agência de viagens na presença física do cliente;

d) Disponibilização de jogos eletrónicos numa sala de jogos na presença física do utilizador.

3. São também excluídos da aplicação do diploma os serviços que não são fornecidos por via eletrónica:
a) Serviços cujo conteúdo é material, mesmo quando impliquem a utilização de dispositivos eletrónicos:
i) Distribuição automática de notas e bilhetes, tais como notas de banco e bilhetes de comboio;

ii) Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos eletrónicos à entrada e ou saída para controlar o acesso e ou garantir o correto pagamento;

b) Serviços off-line: distribuição de CD-ROM ou de software em disquettes;

c) Serviços não fornecidos por intermédio de sistemas eletrónicos de armazenagem e processamento de dados:
i) Serviços de telefonia vocal;

ii) Serviços de telecópia e telex;

iii) Teletexto televisivo;

iv) Serviços prestados por telefonia vocal ou telecópia;

v) Consulta de um médico por telefone ou telecópia;

vi) Consulta de um advogado por telefone ou telecópia;

vii) Marketing direto por telefone ou telecópia.

16. Diretiva n.º 98/48/CE, do Parlamento europeu e do Conselho de 20 de Julho de 1998 que altera a Directiva 98/34/CE relativa a um procedimento de informação no domínio das normas e regulamentações técnicas

Tendo em conta o Tratado que institui a Comunidade Europeia e, nomeadamente, os seus artigos 100ºA e 213º,

Tendo em conta a proposta da Comissão[68],

Tendo em conta o parecer do Comité Económico e Social[69],

Deliberando nos termos do artigo 189ºB do Tratado[70],

1 // Considerando que, para permitir o bom funcionamento do mercado interno, é necessário assegurar, através de uma alteração da Diretiva 98/34/CE[71], a maior transparência das futuras regulamentações nacionais que se aplicarão aos serviços da sociedade da Informação;

2 // Considerando que uma grande variedade de serviços, na aceção dos artigos 59º e 60º do Tratado, vai beneficiar das oportunidades de prestação à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços, abertas pela sociedade da informação;

3 // Considerando que o espaço sem fronteiras internas que constitui o mercado interno permite aos prestadores desses serviços desenvolver as suas atividades transfronteiriças a fim de aumentar a sua competitividade, propiciando assim aos cidadãos novas possibilidades de comunicar e de receber informações sem considerações de fronteiras e aos consumidores novas formas de acesso a bens ou serviços;

---

[68] JO C 307 de 16. 10. 1996, p. 11, e JO C 65 de 28. 2. 1998, p. 12.

[69] JO C 158 de 26. 5. 1997, p. 1.

[70] Parecer do Parlamento Europeu de 16 de Maio de 1997 (JO C 167 de 2. 6. 1997, p. 238), posição comum do Conselho de 26 de Janeiro de 1998 (JO C 62 de 26. 2. 1998, p. 48) e decisão do Parlamento Europeu de 14 de Maio de 1998 (JO C 167 de 1. 6. 1998). Decisão do Conselho de 29 de Junho de 1998.

[71] JO L 204 de 21. 7. 1998, p. 37.

4 // Considerando que o alargamento da Diretiva 98/34/CE não deve obstar a que os Estados-membros tenham em conta as diferentes implicações sociais, societais e culturais inerentes ao advento da sociedade da informação; que, em especial, a utilização das regras processuais previstas nesta diretiva em matéria de serviços da sociedade da informação não deve prejudicar as medidas de política cultural; nomeadamente no domínio audiovisual, que os Estados-membros possam adotar, segundo o direito comunitário, tendo em conta a sua diversidade linguística, as especificidades nacionais e regionais, bem como os seus patrimónios culturais; que o desenvolvimento da sociedade da informação deverá assegurar, de qualquer modo, o correto acesso dos cidadãos europeus ao património cultural europeu fornecido num ambiente digital;

5 // Considerando que a Diretiva 98/34/CE não se destina a ser aplicada a regras nacionais relativas aos direitos fundamentais, como, por exemplo, as regras constitucionais em matéria de liberdade de expressão, e mais precisamente, de liberdade de imprensa; que não se destina igualmente a ser aplicada ao direito penal geral; que, além disso, não se aplica aos acordos de direito privado entre instituições de crédito, nomeadamente aos acordos sobre a realização de pagamentos entre instituições de crédito;

6 // Considerando que o Conselho Europeu realçou a necessidade de criar um quadro jurídico claro e estável a nível comunitário que permita o desenvolvimento da Sociedade da Informação; que o direito comunitário e as disposições relativas ao mercado interno em especial e tanto os princípios do Tratado como o direito derivado constituem já um quadro jurídico de base para o desenvolvimento destes serviços;

7 // Considerando que as regulamentações nacionais existentes aplicáveis aos serviços atuais deverão poder ser adaptadas aos novos serviços da sociedade da informação, quer para assegurar uma melhor proteção dos interesses gerais, quer, pelo contrário, para simplificar essas regulamentações, nos casos em que a sua aplicação seria desproporcionada relativamente aos objetivos visados;

8 // Considerando que, sem coordenação a nível comunitário, esta atividade regulamentar previsível a nível nacional poderia implicar restrições à livre circulação de serviços e à liberdade de estabelecimento,

que provocariam uma refragmentação do mercado interno, uma regulamentação excessiva e incoerências regulamentares;

9 // Considerando a necessidade de uma abordagem coordenada a nível comunitário no tratamento das questões relativas a atividades com conotações eminentemente transnacionais, tais como os novos serviços, a fim de conseguir também uma proteção real e efetiva dos objetivos de interesse geral pertinentes para o desenvolvimento da sociedade da informação;

10 // Considerando que, para os serviços de telecomunicações, existe já uma harmonização a nível comunitário ou, eventualmente, um regime de reconhecimento mútuo e que a legislação comunitária existente prevê adaptações ao desenvolvimento tecnológico e aos novos serviços prestados e que por esse facto, na sua maior parte, as regulamentações nacionais dos serviços de telecomunicações não deverão ser notificadas ao abrigo da presente diretiva, uma vez que decorrerão das exclusões previstas no nº 1 do artigo 10º, ou no ponto 5 do artigo 1º da Diretiva 98/34/CE; que, no entanto, as disposições nacionais que visem especificamente questões não regulamentadas a nível comunitário podem ter influência na livre circulação dos serviços da sociedade da informação e que, nessa medida, devem ser notificadas;

11 // Considerando que para outros domínios da sociedade da informação ainda pouco conhecidos, seria, contudo, prematuro coordenar estas regulamentações através de uma harmonização extensiva ou exaustiva, a nível comunitário, do direito substantivo, dado que a forma e a natureza dos novos serviços não são suficientemente conhecidas, que não existem ainda a nível nacional atividades regulamentares específicas na matéria e que a necessidade e o conteúdo de tal harmonização relativamente ao mercado interno não podem ser definidos nesta fase;

12 // Considerando que é pois necessário preservar o bom funcionamento do mercado interno e prevenir os riscos de refragmentação, prevendo um procedimento de informação, consulta e cooperação administrativa relativo aos novos projetos de regulamentação; que este procedimento contribuirá, nomeadamente, para garantir uma aplicação eficaz do Tratado, em especial dos artigos 52º e 59º ou, se for caso disso, para detetar a necessidade

de assegurar a proteção de um interesse geral a nível comunitário; que, além disso, a melhor aplicação do Tratado proporcionada por tal procedimento de informação terá como consequência reduzir a necessidade de regulamentações comunitárias ao estritamente necessário e proporcional em relação ao mercado interno e à proteção de objetivos de interesse geral; que este procedimento de informação permitirá, por último, uma melhor exploração, pelas empresas, das vantagens do mercado interno;

13 // Considerando que a Diretiva 98/34/CE visa os mesmos objetivos e que este procedimento, além de eficaz, é o mais aperfeiçoado em função desses objetivos; que os resultados da aplicação desta diretiva e os procedimentos nela previstos se coadunam com os projetos de regras relativas aos serviços da sociedade da informação; que o procedimento previsto na diretiva está atualmente bem integrado a nível das administrações nacionais;

14 // Considerando por outro lado que, nos termos do artigo 7ºA do Tratado, o mercado interno compreende um espaço sem fronteiras internas no qual é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais e que a Diretiva 98/34/CE prevê apenas um processo de cooperação administrativa, sem harmonização de regras materiais;

15 // Considerando, por conseguinte, que a alteração da Diretiva 98/34/CE para a aplicar aos projetos de regulamentação relativos aos serviços da sociedade da informação constitui a abordagem mais adequada para dar uma resposta eficaz às necessidades de transparência no mercado interno no que se refere ao quadro jurídico daqueles serviços;

16 // Considerando que será preciso prever uma notificação, nomeadamente das regras que poderão vir a evoluir no futuro; que, dada a sua diversidade e o seu desenvolvimento futuro, os serviços mais suscetíveis de necessitar e de gerar novas regras e regulamentações são os serviços prestados à distância, por via eletrónica, e mediante pedido individual de um destinatário de serviços (serviços da sociedade da informação); que, por isso, se deve prever a notificação dos projetos de regras e regulamentações relativos a esses serviços;

17 // Considerando que, desta forma, deverão ser comunicadas as regras específicas relativas ao acesso aos serviços suscetíveis de serem prestados segundo as regras acima definidas e ao seu exercício, mesmo que essas regras estejam incluídas numa regulamentação com um objetivo mais geral; que, todavia, as regulamentações gerais que não prevejam qualquer disposição que vise especificamente esses serviços não deverão ser notificadas;

18 // Considerando que, por regras relativas ao acesso aos serviços e ao seu exercício se deve entender as que fixam exigências relativas aos serviços da sociedade da informação, como as relativas aos prestadores, aos serviços e aos destinatários de serviços, que dizem respeito a uma atividade económica suscetível de ser prestada por via eletrónica, à distância e mediante pedido individual do destinatário do serviço; que, consequentemente, ficarão por exemplo abrangidas as regras relativas ao estabelecimento dos prestadores destes serviços e, em especial, as relativas ao regime de autorização ou de licenças; que se considera como regra destinada especificamente aos serviços da sociedade da informação uma disposição que vise estes últimos, ainda que contida numa regulamentação de carácter geral; que, em contrapartida, não se terão em vista medidas relativas, tanto direta como individualmente, a determinados destinatários especiais (como, por exemplo, licenças em matéria de telecomunicações);

19 // Considerando que por serviços se deve entender, nos termos do artigo 60º do Tratado interpretado pela jurisprudência do Tribunal de Justiça, uma prestação realizada normalmente mediante remuneração; que essa característica não está presente nas atividades que o Estado desempenha sem contrapartida económica no âmbito da sua missão, nomeadamente nos domínios social, cultural, educativo e judiciário; que, por esse facto, as regras nacionais relativas a essas atividades não estão abrangidas pela definição prevista no artigo 60º do Tratado e não recaem, por conseguinte, no âmbito de aplicação da presente diretiva;

20 // Considerando que a presente diretiva não prejudica o âmbito de aplicação da Diretiva 89/552/CEE do Conselho, de 3 de Outubro de 1989, relativa à coordenação de certas disposições legislativas, regulamentares

e administrativas dos Estados-membros relativas ao exercício de atividades de radiodifusão televisiva[72], corra a redação que lhe foi dada pela Diretiva 97/36/CE do Parlamento Europeu e do Conselho[73], ou de eventuais futuras alterações desta diretiva;

21 // Considerando que, de qualquer forma, não estão abrangidos pela presente diretiva os projetos de disposições nacionais destinadas a transpor o conteúdo das diretivas comunitárias em vigor ou a ser adotadas, uma vez que são já objeto de um exame específico; que, consequentemente, não ficarão abrangidas pelo âmbito de aplicação da presente diretiva nem as regulamentações nacionais de transposição da Diretiva 89/552/CEE, com a redação que lhe foi dada pela Diretiva 97/36/CE, ou eventuais futuras alterações desta diretiva, nem as regulamentações nacionais de transposição ou adotadas sucessivamente no contexto da Diretiva 97/13/CE do Parlamento Europeu do Conselho, de 10 de Abril de 1997, relativa a um quadro comum para as autorizações gerais e as licenças individuais no sector dos serviços de telecomunicações[74];

22 // Considerando, além disso, que é importante prever casos excecionais em que regulamentações nacionais relativas aos serviços da sociedade da informação possam ser adotadas imediatamente e que é igualmente importante admitir esta possibilidade unicamente por motivos urgentes relacionados com situações graves e imprevisíveis, nomeadamente, situações não evidentes anteriormente e cuja origem não é imputável a uma ação das autoridades do Estado-membro em questão, no intuito de não comprometer a finalidade de consulta prévia e de cooperação administrativa inerente à presente diretiva;

23 // Considerando que é conveniente que um Estado-membro adie por doze meses - eventualmente por dezoito meses, em caso de posição comum do Conselho - a adoção de um projeto de regra relativa aos serviços apenas na hipótese em que o projeto diga respeito a uma matéria abrangida por uma proposta de diretiva, de regulamento ou de decisão já apresentada pela Comissão ao Conselho; que esta obrigação de adiamento só poderá ser contraposta pela Comissão ao Estado-membro

[72] *JO L 298 de 17. 10. 1989, p. 23.*
[73] *JO L 202 de 30. 7. 1997, p. 1.*
[74] *JO L 117 de 7. 5. 1997, p. 15.*

em questão no caso de o projeto de regra nacional prever disposições não conformes com o conteúdo da proposta apresentada pela Comissão;

24 // Considerando que a definição do quadro de informação e de consulta a nível comunitário estabelecido pela presente diretiva constitui uma condição prévia para uma participação coerente e eficaz da Comunidade Europeia no tratamento das questões relacionadas com os aspetos regulamentares dos serviços da sociedade da informação no contexto internacional;

25 // Considerando que é conveniente que, no âmbito do funcionamento da Diretiva 98/34/CE, o Comité previsto no artigo 5º se reúna especificamente para analisar as questões relativas aos serviços da sociedade da informação;

26 // Considerando que, na mesma perspetiva, se deve recordar que, sempre que uma medida nacional tenha de ser notificada igualmente na fase de projeto por força de outro ato comunitário, o Estado-membro em questão pode fazer uma comunicação única ao abrigo desse ato, referindo que essa comunicação constitui igualmente uma comunicação na aceção da presente diretiva;

27 // Considerando que a Comissão apreciará regularmente a evolução do mercado de novos serviços no âmbito da sociedade da informação, em especial no que diz respeito à convergência entre as telecomunicações, as tecnologias da informação e os meios de comunicação, promovendo designadamente estudos e, se necessário, adotando iniciativas tendentes a adaptar atempadamente a regulamentação, com o objetivo de favorecer o desenvolvimento de novos serviços a nível europeu,

ADOTARAM A PRESENTE DIRETIVA:

Artigo 1.º
A Diretiva 98/34/CE é alterada do seguinte modo:
1. O título da diretiva passa a ter a seguinte redação:
«Diretiva do Parlamento Europeu e do Conselho relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação».

2. O artigo 1º é alterado do seguinte modo:
a) É aditado um novo ponto 2:
«2. "serviço": qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços.
Para efeitos da presente definição, entende-se por:
- "à distância": um serviço prestado sem que as partes estejam simultaneamente presentes,
- "por via eletrónica": um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos,
- "mediante pedido individual de um destinatário de serviços": um serviço fornecido por transmissão de dados mediante pedido individual.
No anexo V figura uma lista indicativa dos serviços não incluídos nesta definição.
A presente diretiva não é aplicável:
- aos serviços de radiodifusão sonora,
- aos serviços de radiodifusão televisiva referidos na alínea a) do artigo 1º da Diretiva 89/552/CEE[75].

b) Os pontos 2 e 3 passam respetivamente a 3 e 4;

c) É aditado um novo ponto 5:
«5. "regra relativa aos serviços": um requisito de natureza geral relativo ao acesso às atividades de serviços referidas no nº 2 do presente artigo e ao seu exercício, nomeadamente as disposições relativas ao prestador de serviços, aos serviços e ao destinatário de serviços, com exclusão das regras que não visem especificamente os serviços definidos nessa mesma disposição.
A presente diretiva não é aplicável a regras relativas a questões sujeitas à regulamentação comunitária em matéria de serviços de telecomunicações definidos na Diretiva 90/387/CEE[76].

---

[75] JO L 298 de 17. 10. 1989, p. 23. Diretiva com a redação que lhe foi dada pela Diretiva 97/36/CE (JO L 202 de 30. 7. 1997, p. 1).»;
[76] JO L 192 de 24. 7. 1990, p. 1. Diretiva com a redação que lhe foi dada pela Diretiva 97/51/CE (JO L 295 de 29. 10. 1997, p. 23).

A presente diretiva não é aplicável a regras relativas a questões sujeitas à regulamentação comunitária em matéria de serviços financeiros enumerados exemplificativamente no Anexo VI da presente diretiva.
A presente diretiva não é aplicável às regras enunciadas pelos ou para os mercados regulamentados na aceção da Diretiva 93/22/CE, outros mercados ou órgãos que efetuem operações de compensação ou de liquidação desses mercados, com exceção do nº 3 do artigo 8º da presente diretiva.
Para efeitos da presente definição:
- considera-se que uma regra tem em vista especificamente os serviços da sociedade da informação sempre que, no que diz respeito à sua motivação e ao texto do seu articulado, tenha como finalidade e objeto específicos, na totalidade ou em determinadas disposições pontuais, regulamentar de modo explícito e circunscrito esses serviços,
- não se considera que uma regra tem em vista especificamente os serviços da sociedade da informação se apenas disser respeito a esses serviços de modo implícito ou incidente;

d) Os pontos 4 a 8 passam, respetivamente, a 6 e a 10;

e) O ponto 9 passa a 11 com a seguinte redação:
«11. "regra técnica": uma especificação técnica, outro requisito ou uma regra relativa aos serviços, incluindo as disposições administrativas que lhes são aplicáveis e cujo cumprimento seja obrigatório de jure ou de facto, para a comercialização, a prestação de serviços, o estabelecimento de um operador de serviços ou a utilização num Estado-membro ou numa parte importante desse Estado, assim como, sob reserva das disposições referidas no artigo 10º, qualquer disposição legislativa, regulamentar ou administrativa dos Estados-membros que proíba o fabrico, a importação, a comercialização, ou a utilização de um produto ou a prestação ou utilização de um serviço ou o estabelecimento como prestador de serviços.
Constituem nomeadamente regras técnicas de facto:
- as disposições legislativas, regulamentares ou administrativas de um Estado-Membro que remetam para especificações técnicas, outros requisitos ou regras relativas aos serviços, ou para códigos profissionais ou de boa prática que se refiram a especificações técnicas, a outros requisitos ou a regras relativas aos serviços, cuja observância confira uma presunção de conformidade com as prescrições estabelecidas pelas referidas disposições legislativas, regulamentares ou administrativas,

- os acordos voluntários em que uma entidade pública seja parte contratante e que visem, numa perspetiva de interesse geral, a observância de especificações técnicas, de outros requisitos ou de regras relativas aos serviços, com exceção dos cadernos de encargos dos contratos públicos,
- as especificações técnicas, outros requisitos ou regras relativas aos serviços, relacionados com medidas de carácter fiscal ou financeiro que afetem o consumo de produtos ou de serviços, incitando à observância dessas especificações técnicas, outros requisitos, ou regras relativas aos serviços; não se incluem as especificações técnicas, outros requisitos ou as regras relativas aos serviços relacionados com os regimes nacionais de segurança social.
São abrangidas as regras técnicas definidas pelas autoridades designadas pelos Estados-membros e incluídas numa lista a elaborar pela Comissão em 5 de Agosto de 1999 no âmbito do comité previsto no artigo 5º
A alteração desta lista efetuar-se-á segundo o mesmo processo.»;

f) O ponto 10 passa a ponto 12 e o seu primeiro parágrafo passa a ter a seguinte redação:
«12. "projeto de regra técnica": o texto de uma especificação técnica, de outro requisito ou de uma regra relativa aos serviços, incluindo disposições administrativas, elaborado com o objetivo de a adotar ou de a fazer adotar como regra técnica, e que se encontre numa fase de preparação que permita ainda a introdução de alterações substanciais.»

3. O artigo 6º é alterado do seguinte modo:
a) Ao nº 1 é aditado o seguinte parágrafo:
«O comité reúne-se com uma composição específica para analisar as questões relativas aos serviços da sociedade da informação.»;

b) É aditado o seguinte parágrafo:
«8. No que respeita às regras aplicáveis aos serviços, a Comissão e o comité podem consultar pessoas singulares ou coletivas do sector industrial ou do meio académico, e, quando possível, corpos representativos com competência para emitir um parecer sobre os objetivos e as consequências sociais e societais de qualquer projeto de regra relativa aos serviços, e ter em conta esse parecer sempre que o fizerem.»

4. No artigo 8º, o nº 1, sexto parágrafo, passa a ter a seguinte redação:
«No que respeita às especificações técnicas, outros requisitos ou

regras relativas aos serviços referidas no ponto 11, segundo parágrafo, terceiro travessão, do artigo 1º, as observações ou os pareceres circunstanciados da Comissão ou dos Estados-membros apenas podem incidir sobre os aspetos suscetíveis de entravar as trocas comerciais ou, no que diz respeito às regras relativas aos serviços, a livre circulação dos serviços ou a liberdade de estabelecimento dos operadores de serviços, e não sobre a vertente fiscal ou financeira da medida em questão.»

5. O artigo 9º é alterado do seguinte modo:
a) Os nºs 2 e 3 passam a ter a seguinte redação:
«2. Os Estados-membros adiarão:
- por quatro meses a adoção de um projeto de regra técnica sob a forma de acordo voluntário na aceção do ponto 11, segundo parágrafo, segundo travessão, do artigo 1º,
- por seis meses, sem prejuízo do disposto nos nºs 3, 4 e 5, a adoção de qualquer outro projeto de regra técnica (com exclusão dos projetos relativos aos serviços),
a contar da data de receção pela Comissão da comunicação referida no nº 1 do artigo 8º se, no prazo de três meses subsequentes a essa data, a Comissão ou outro Estado-membro emitir um parecer circunstanciado segundo o qual a medida prevista apresenta aspetos que podem eventualmente criar obstáculos à livre circulação das mercadorias no âmbito do mercado interno;
- por quatro meses, sem prejuízo do disposto nos nºs 4 e 5, a adoção de um projeto de regra relativa aos serviços, a contar da data de receção pela Comissão da comunicação referida no nº 1 do artigo 8º, se, no prazo de três meses subsequentes a essa data, a Comissão ou outro Estado-membro emitir um parecer circunstanciado segundo o qual a medida prevista apresenta aspetos que podem eventualmente criar obstáculos à livre circulação dos serviços ou à liberdade de estabelecimento dos operadores de serviços no âmbito do mercado interno.
Quanto aos projetos de regras relativas aos serviços, os pareceres circunstanciados da Comissão ou dos Estados-membros não podem prejudicar as medidas de política cultural, nomeadamente no domínio do audiovisual, que os Estados possam adotar, nos termos do direito comunitário, tendo em conta a sua diversidade linguística, as especificidades nacionais e regionais, e os seus patrimónios culturais.

O Estado-membro em causa apresentará à Comissão um relatório sobre o seguimento que pretende dar a esses pareceres circunstanciados. A Comissão comentará essa reação.
No que respeita às regras relativas aos serviços, o Estado-membro em questão deverá indicar, sempre que for oportuno, os motivos pelos quais não é possível ter em conta os pareceres circunstanciados.
3. Os Estados-membros adiarão a adoção de um projeto de regra técnica, com exclusão dos projetos de regras relativas aos serviços, por doze meses a contar da data de receção pela Comissão da comunicação a que se refere o nº 1 do artigo 8º se, no prazo de três meses subsequentes a essa data, a Comissão manifestar a intenção de propor ou adotar uma diretiva, um regulamento ou uma decisão nessa matéria, nos termos do artigo 189º do Tratado.»;

b) O nº 7 passa a ter a seguinte redação:
«7. Os nºs 1 a 5 não se aplicam sempre que um Estado-membro:
- por razões urgentes, resultantes de uma situação grave e imprevisível que envolva a defesa da saúde das pessoas e dos animais, a preservação das plantas ou a segurança e, no que se refere às regras relativas aos serviços, a ordem pública, nomeadamente a proteção dos menores, tenha de elaborar, com a maior brevidade, regras técnicas a adotar e aplicar de imediato, sem possibilidade de proceder a uma consulta, ou
- por razões urgentes, resultantes de uma situação grave que envolva a proteção da segurança e integridade do sistema financeiro, nomeadamente tendo em vista a defesa dos depositantes, investidores e segurados, tenha de adotar e aplicar de imediato regras relativas aos serviços financeiros.
Na comunicação referida no artigo 8º, o Estado-membro deverá indicar os motivos que justificam a urgência das medidas em questão. A Comissão pronunciar-se-á sobre essa comunicação no mais curto prazo possível, tomará as medidas adequadas em caso de recurso abusivo a este procedimento e manterá também o Parlamento Europeu informado.»

6. O artigo 10º é alterado do seguinte modo:
a) O primeiro e segundo travessões do nº 1 passam a ter a seguinte redação:
«- deem cumprimento aos atos comunitários vinculativos cujo efeito seja

a adoção de especificações técnicas ou de regras relativas aos serviços,
- observem os compromissos decorrentes de um acordo internacional cujo efeito seja a adoção de especificações técnicas ou de regras relativas aos serviços e que sejam comuns a toda a Comunidade,»;

b) No nº 1, o sexto travessão passa a ter a seguinte redação:
«- se limitem a alterar uma regra técnica na aceção do ponto 11, do artigo 1º, de acordo com um pedido da Comissão tendo em vista eliminar um entrave às trocas comerciais ou, quanto às regras relativas aos serviços, à livre circulação dos serviços ou à liberdade de estabelecimento dos operadores de serviços.»;

c) Os nºs 3 e 4 passam a ter a seguinte redação:
«3. Os nºs 3 a 6 do artigo 9º não são aplicáveis aos acordos voluntários previstos no ponto 11, segundo parágrafo, segundo travessão do artigo 1º
4. O artigo 9º não é aplicável às especificações técnicas ou outros requisitos, nem às regras relativas aos serviços a que se refere o ponto 11, segundo parágrafo, terceiro travessão, do artigo 1º»;

7. São aditados os anexos V e VI que constam do anexo da presente diretiva.

Artigo 2.º
1. Os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva o mais tardar em 5 de Agosto de 1999. Do facto informarão imediatamente a Comissão.
Quando os Estados-membros adotarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência na publicação oficial. As modalidades dessa referência serão adotadas pelos Estados-membros.

2. Os Estados-membros comunicarão à Comissão o texto das principais disposições de direito interno que adotem no domínio regido pela presente diretiva.

Artigo 3.º
O mais tardar dois anos a contar da data prevista no nº 1, primeiro parágrafo, do artigo 2º, a Comissão apresentará ao Parlamento Europeu e

ao Conselho, uma avaliação da aplicação da Diretiva 98/34/CE, em função, nomeadamente, da evolução tecnológica e do mercado dos serviços referidos no nº 2 do artigo 1º O mais tardar três anos a contar da data prevista no nº 1, primeiro parágrafo, do artigo 2º da presente diretiva, a Comissão apresentará eventualmente propostas de alteração da diretiva ao Parlamento Europeu e ao Conselho.
Para esse efeito, a Comissão tomará em consideração as observações que os Estados-membros lhe possam comunicar.

Artigo 4.º
A presente diretiva entra em vigor na data da sua publicação no Jornal Oficial das Comunidades Europeias.

Artigo 5.º
Os Estados-membros são os destinatários da presente diretiva.
Feito em Bruxelas, em 20 de Julho de 1998.

Pelo Parlamento Europeu
O Presidente
J. M. GIL-ROBLES
Pelo Conselho
O Presidente
W. MOLTERER

ANEXO
ANEXO V

Lista indicativa de serviços não abrangidos pelo artigo 1º, ponto 2, segundo parágrafo
1. Serviços que não são prestados "à distância"
Serviços prestados na presença física do prestador e do destinatário, mesmo que impliquem a utilização de dispositivos eletrónicos:
a) Exames ou tratamentos num consultório médico por meio de equipamentos eletrónicos mas na presença física do paciente;

b) Consulta de um catálogo eletrónico num estabelecimento comercial na presença física do cliente;

c) Reserva de um bilhete de avião de uma rede de computadores numa

agência de viagem na presença física do cliente;
d) Disponibilização de jogos eletrónicos numa sala de jogos na presença física do utilizador.

2. Serviços que não são fornecidos "por via eletrónica"
- Serviços cujo conteúdo é material mesmo quando impliquem a utilização de dispositivos eletrónicos) Distribuição automática de notas e bilhetes (notas de banco, bilhetes de comboio);
b) Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos eletrónicos à entrada e/ou saída para controlar o acesso e/ou garantir o correto pagamento;
- Serviços off-line: distribuição de CD-ROM ou de software em disquetes,
- Serviços não fornecidos por intermédio de sistemas eletrónicos de armazenagem e processamento de dados:
a) Serviços de telefonia vocal;

b) Serviços de telecópia/telex;

c) Serviços prestados por telefonia vocal ou telecópia;

d) Consulta de um médico por telefone/telecópia;

e) Consulta de um advogado por telefone/telecópia;

f) Marketing direto por telefone/telecópia;

3. Serviços que não são fornecidos "a pedido individual"
Serviços fornecidos por envio de dados sem pedido individual e destinados à receção simultânea por um número ilimitado de destinatários (transmissão de "ponto para multi-ponto")
a) Serviços de radiodifusão televisiva (incluindo o quase vídeo a pedido) previstos no artigo 1º, alínea a), da Diretiva 89/552/CEE;

b) Serviços de radiodifusão sonora;

c) Teletexto (televisivo).

ANEXO VI

Lista indicativa dos serviços financeiros previstos no artigo 1º, ponto 5, terceiro parágrafo
- Serviços de investimento
- Operações de seguro e resseguro
- Serviços bancários
- Operações relativas aos fundos de pensões
- Serviços relativos a operações a prazo ou em opção.

Estes serviços compreendem em especial:

a) Os serviços de investimento referidos no anexo da Diretiva 93/22/CEE[77], os serviços de empresas de investimento coletivo,

b) Os serviços abrangidos pelas atividades que beneficiam do reconhecimento mútuo contemplados no anexo da Diretiva 89/646/CEE[78],

c) As operações respeitantes às atividades de seguro e resseguro referidas:
- no artigo 1.º da Diretiva 73/239/CEE[79],
- no anexo da Diretiva 79/267/CEE[80],
- na Diretiva 94/225/CEE[81],
- nas Diretivas 92/49/CEE[82] e 92/96/CEE[83].

---

[77] JO L 141 de 11. 6. 1993, p. 27.

[78] JO L 386 de 30. 12. 1989, p. 1. Diretiva com a redação que lhe foi dada pela Diretiva 92/30/CEE (JO L 110 de 28. 4. 1992, p. 52).

[79] JO L 228 de 16. 8. 1973, p. 3. Diretiva com a última redação que lhe foi dada pela Diretiva 92/49/CEE (JO L 228 de 11. 8. 1992, p. 1).

[80] JO L 63 de 13. 3. 1979, p. 1. Diretiva com a última redação que lhe foi dada pela Diretiva 90/619/CEE (JO L 330 de 29. 11. 1990, p. 50).

[81] JO 56 de 4. 4. 1964, p. 878/64. Diretiva com a última redação que lhe foi dada pelo Ato de Adesão de 1973.

[82] JO L 228 de 11. 8. 1992, p. 1.

[83] JO L 360 de 9. 12. 1992, p. 1.

17. Lei nº 109/2009, de 15 de Setembro,
aprova a lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa

CAPÍTULO I
OBJETO E DEFINIÇÕES

Artigo 1.º Objeto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro[84], relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Artigo 2.º Definições

Para efeitos da presente lei, considera-se:

a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

---

[84] Vd. Diretiva 2013/40/EU do Parlamento e do Conselho, de 12 de Agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.

c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

d) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores;

e) «Interceção», o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respetivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função eletrónica.

CAPÍTULO II
DISPOSIÇÕES PENAIS MATERIAIS

Artigo 3.º Falsidade informática

1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que

estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2. Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3. Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

Artigo 4.º Dano relativo a programas ou outros dados informáticos

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

2. A tentativa é punível.

3. Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.

4. Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5. Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

6. Nos casos previstos nos n.ºs 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 5.º Sabotagem informática
1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2. Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3. Nos casos previstos no número anterior, a tentativa não é punível.

4. A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5. A pena é de prisão de 1 a 10 anos se:
a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 6.º Acesso ilegítimo
1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3. A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4. A pena é de prisão de 1 a 5 anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5. A tentativa é punível, salvo nos casos previstos no n.º 2.

6. Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa.

Artigo 7.º Interceção ilegítima
1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão

até 3 anos ou com pena de multa.

2. A tentativa é punível.

3. Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no mesmo número.

Artigo 8.º Reprodução ilegítima de programa protegido
1. Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.

2. Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3. A tentativa é punível.

Artigo 9.º Responsabilidade penal das pessoas coletivas e entidades equiparadas
As pessoas coletivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

Artigo 10.º Perda de bens
1. O tribunal pode decretar a perda a favor do Estado dos objetos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.

2. À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam suscetíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto-Lei n.º 11/2007, de 19 de Janeiro.

CAPÍTULO III
DISPOSIÇÕES PROCESSUAIS

Artigo 11.º Âmbito de aplicação das disposições processuais
1. Com exceção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:
a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

2. As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

Artigo 12.º Preservação expedita de dados
1. Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2. A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

3. A ordem de preservação discrimina, sob pena de nulidade:
a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.

4. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5. A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 13.º Revelação expedita de dados de tráfego
Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Artigo 14.º Injunção para apresentação ou concessão do acesso a dados
1. Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2. A ordem referida no número anterior identifica os dados em causa.

3. Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4. O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:
a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

6. Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista.

7. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 15.º Pesquisa de dados informáticos
1. Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2. O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3. O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:
a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4. Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:
a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5. Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.

6. À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.

Artigo 16.º Apreensão de dados informáticos
1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2. O órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

4. As apreensões efetuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5. As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das atividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

6. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

7. A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:
a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8. No caso da apreensão efetuada nos termos da alínea b) do número anterior, a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Artigo 17.º Apreensão de correio eletrónico
e registos de comunicações de natureza semelhante
Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 18.º Interceção de comunicações
1. É admissível o recurso à interceção de comunicações em processos relativos a crimes:
a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

2. A interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

3. A interceção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de

dados de tráfego, devendo o despacho referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.

4. Em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

Artigo 19.º Ações encobertas
1. É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:
a) Os previstos na presente lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

2. Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.

CAPÍTULO IV
COOPERAÇÃO INTERNACIONAL

Artigo 20.º Âmbito da cooperação internacional
As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime, de acordo com as normas sobre

transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro.

Artigo 21.º Ponto de contacto permanente para a cooperação internacional

1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.

2. Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3. A assistência imediata prestada por este ponto de contacto permanente inclui:

a) A prestação de aconselhamento técnico a outros pontos de contacto;

b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução.

4. Sempre que atue ao abrigo das alíneas b) a d) do número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

Artigo 22.º Preservação e revelação expeditas de dados informáticos em cooperação internacional

1. Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2. A solicitação especifica:
a) A autoridade que pede a preservação;

b) A infração que é objeto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;
c) Os dados informáticos a conservar e a sua relação com a infração;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) A necessidade da medida de preservação; e

f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

3. Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.

4. A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.

5. A ordem de preservação especifica, sob pena de nulidade:
a) A natureza dos dados;

b) Se forem conhecidos, a origem e o destino dos mesmos; e

c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.

6. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.

7. A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

8. Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adoção de uma decisão final sobre o pedido.

9. Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos:
a) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 13.º a 17.º;

b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 13.º

10. A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efetuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11. O disposto nos n.ºs 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas.

Artigo 23.º Motivos de recusa
1. A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:
a) Os dados informáticos em causa respeitarem a infração de natureza política ou infração conexa segundo as conceções do direito português;

b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos;

c) O Estado terceiro requisitante não oferecer garantias adequadas de proteção dos dados pessoais.

2. A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 24.º Acesso a dados informáticos em cooperação internacional
1. Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.

2. A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável.

3. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

Artigo 25.º Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento
As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre

transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro, podem:
a) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis;

b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Artigo 26.º Interceção de comunicações em cooperação internacional
1. Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a interceção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal interceção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante.

2. É competente para a receção dos pedidos de interceção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização.

3. O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido.

4. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

CAPÍTULO V
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Artigo 27.º Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses
1. Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:

a) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;

b) Cometidos em benefício de pessoas coletivas com sede em território português;

c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou
d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

2. Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respetivas ações, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infração, tendo em vista centralizá-lo num só deles.

3. A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:
a) O local onde foi praticada a infração;

b) A nacionalidade do autor dos factos; e

c) O local onde o autor dos factos foi encontrado.

4. São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal.

5. Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente atuou e o local onde está fisicamente instalado o sistema informático

visado com a sua atuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 28.º Regime geral aplicável
Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respetivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto.

Artigo 29.º Competência da Polícia Judiciária para a cooperação internacional
A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.
Artigo 30.º Proteção de dados pessoais
O tratamento de dados pessoais ao abrigo da presente lei efetua-se de acordo com o disposto na Lei n.º 67/98, de 26 de Outubro, sendo aplicável, em caso de violação, o disposto no respetivo capítulo vi.

Artigo 31.º Norma revogatória
É revogada a Lei n.º 109/91, de 17 de Agosto.

Artigo 32.º Entrada em vigor
A presente lei entra em vigor 30 dias após a sua publicação.
Aprovada em 23 de Julho de 2009.
O Presidente da Assembleia da República,
Jaime Gama.
Promulgada em 29 de Agosto de 2009.
Publique-se. O Presidente da República,
Aníbal Cavaco Silva.
Referendada em 31 de Agosto de 2009.
O Primeiro-Ministro,
José Sócrates Carvalho Pinto de Sousa.

18. Decisão Quadro nº 2005/222/JAI
relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre cibercrime do Conselho da Europa (Revogada)[85]

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 29.o, a alínea a) do n.o 1 do artigo 30.o, a alínea e) do n.º 1 do artigo 31.o e a alínea b) do n.º 2 do artigo 34.o,

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Parlamento Europeu[86],

Considerando o seguinte:

1 // A presente decisão-quadro tem por objetivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.

2 // Há provas de ataques contra os sistemas de informação, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação que constituem a infraestrutura vital dos Estados-Membros. Esta ameaça poderá comprometer a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia.

3 // Uma resposta eficaz a essas ameaças pressupõe uma abordagem

---

[85] Pela Diretiva 2013/40/CE do Parlamento Europeu e do Conselho, relativa a ataques contra os sistemas de informação.

[86] JO C 300 E de 11.12.2003, p. 26.

global em matéria de segurança das redes e da informação, como foi sublinhado no Plano de Ação «eEurope», na Comunicação da Comissão intitulada «Segurança das redes e da informação: proposta de abordagem de uma política europeia» e na Resolução do Conselho de 28 de Janeiro de 2002, sobre uma abordagem comum e ações específicas no domínio da segurança das redes e da informação[87].

4 // A necessidade de reforçar a sensibilização para os problemas associados à segurança da informação e de fornecer assistência prática foi igualmente sublinhada pela Resolução do Parlamento Europeu de 5 de Setembro de 2001.

5 // As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio.

6 // O Plano de Ação do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amesterdão relativas à criação de um espaço de liberdade, de segurança e de justiça[88], o Conselho Europeu de Tampere, de 15 e 16 de Outubro de 1999, o Conselho Europeu de Santa Maria da Feira, de 19 e 20 de Junho de 2000, o Painel de Avaliação da Comissão e a Resolução do Parlamento Europeu de 19 de Maio de 2000 mencionam ou requerem medidas legislativas contra a criminalidade de alta tecnologia, nomeadamente definições, incriminação e sanções comuns.

7 // É necessário completar o trabalho realizado pelas organizações internacionais, especialmente ao nível do Conselho da Europa, no domínio da aproximação do direito penal e os trabalhos do G8 sobre cooperação

[87] JO C 43 de 16.2.2002, p. 2.

[88] JO C 19 de 23.1.1999, p. 1.

transnacional no âmbito da criminalidade de alta tecnologia, propondo uma abordagem comum neste domínio ao nível da União Europeia.

Este pedido foi desenvolvido na Comunicação que a Comissão dirigiu ao Conselho, ao Parlamento Europeu, ao Comité Económico reforçando a segurança das infraestruturas da informação e lutando contra a cibercriminalidade.

8 // As disposições de direito penal em matéria de ataques contra os sistemas de informação devem ser harmonizadas, a fim de assegurar a melhor cooperação policial e judiciária possível no que diz respeito às infrações penais associadas a este tipo de ataques e contribuir para a luta contra a criminalidade organizada e o terrorismo.

9 // Todos os Estados-Membros ratificaram a Convenção do Conselho da Europa, de 28 de Janeiro de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Os dados de carácter pessoal, tratados no contexto da aplicação da presente decisão-quadro, serão protegidos em conformidade com os princípios estabelecidos na referida Convenção.

10 // É importante estabelecer definições comuns neste domínio, especialmente em relação aos sistemas de informação e aos dados informáticos, a fim de assegurar uma abordagem coerente da aplicação da presente decisão-quadro nos Estados-Membros.

11 // É necessário adotar uma abordagem comum para os elementos constitutivos das infrações penais, prevendo infrações comuns por acesso ilegal a determinado sistema de informação, por interferência ilegal no sistema e por interferência ilegal nos dados.

12 // No interesse do combate à criminalidade informática, cada Estado-Membro deverá assegurar uma cooperação judiciária eficaz no que diz respeito às infrações baseadas nos tipos de comportamento a que se referem os artigos 2.º, 3.º, 4.º e 5.º.

13 // É necessário evitar uma incriminação exorbitante, nomeadamente de casos insignificantes, bem como a incriminação de titulares de direitos e de pessoas autorizadas.

14 // É necessário que os Estados-Membros estabeleçam sanções para combater os ataques contra os sistemas de informação. Essas sanções deverão ser efetivas, proporcionadas e dissuasivas.

15 // É adequado prever penas mais severas nos casos em que um ataque contra determinado sistema de informação tenha sido praticado no âmbito de uma organização criminosa, tal como definida na Acão Comum 98/733/JAI do Conselho, de 21 de Dezembro de 1998, relativa à incriminação da participação numa organização criminosa nos Estados-Membros da União Europeia[89]. É igualmente adequado prever penas mais severas quando um tal ataque tiver causado danos graves ou lesado interesses essenciais.

16 // Deverão ser igualmente adotadas medidas de cooperação entre os Estados-Membros, a fim de assegurar uma ação eficaz contra os ataques que visem os sistemas de informação. Os Estados-Membros devem, pois, recorrer à atual rede de pontos de contacto operacionais referida na Recomendação do Conselho, de 25 de Junho de 2001, relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia[90], para efeitos de troca de informações.

17 // Atendendo a que os objetivos da presente decisão-quadro, a saber, garantir que os ataques contra os sistemas de informação sejam puníveis em todos os Estados-Membros com sanções penais efetivas, proporcionadas e dissuasivas, bem como melhorar e favorecer a cooperação judiciária, suprimindo potenciais dificuldades, não podem ser suficientemente realizados pelos Estados-Membros, já que as normas devem ser comuns e compatíveis, e podem, pois, ser melhor alcançados ao nível da União, esta pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.o do Tratado CE. Em conformidade com o princípio da proporcionalidade consagrado neste mesmo artigo, a presente decisão-quadro não excede o necessário para alcançar aqueles objetivos.

18 // A presente decisão-quadro respeita os direitos fundamentais e os princípios reconhecidos pelo artigo 6.º do Tratado União Europeia

[89] *JO L 351 de 29.12.1998, p. 1.*

[90] *JO C 187 de 3.7.2001, p. 5.*

e refletidos na Carta dos Direitos Fundamentais da União Europeia, designadamente nos capítulos II e VI,

ADOPTOU A PRESENTE DECISÃO-QUADRO:

Artigo 1.º Definições
Para efeitos da presente decisão-quadro, entende-se por:
a) «Sistema de informação», qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos, de forma a serem processados num sistema de informação, nomeadamente um programa capaz de permitir que um sistema de informação execute uma dada função;

c) «Pessoa coletiva», qualquer entidade que beneficie desse estatuto por força do direito aplicável, com exceção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público;

d) «Não autorizado», acesso ou interferência não consentidos pelo proprietário, por outro titular do direito do sistema ou de parte dele, ou não permitidos nos termos do direito nacional.

Artigo 2.º Acesso ilegal aos sistemas de informação
1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional, não autorizado, à totalidade ou a parte de um sistema de informação seja punível como infração penal, pelo menos nos casos que não sejam de menor gravidade.

2. Os Estados-Membros podem decidir que os comportamentos referidos no n.º 1 são puníveis apenas quando a infração tiver sido cometida em violação de uma medida de segurança.

Artigo 3.º Interferência ilegal no sistema
Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessíveis os dados informáticos, seja punível como infração penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 4.º Interferência ilegal nos dados
Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis os dados informáticos de um sistema de informação seja punível como infração penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 5.º Instigação, auxílio, cumplicidade e tentativa
1. Cada Estado-Membro deve assegurar que a instigação, o auxílio e a cumplicidade na prática de alguma das infrações referidas nos artigos 2.o, 3.o e 4.o sejam puníveis como infração penal.

2. Cada Estado-Membro deve assegurar que a tentativa de prática das infrações referidas nos artigos 2.º, 3.º e 4.º seja punível como infração penal.

3. Cada Estado-Membro pode decidir não aplicar o n.º 2 relativamente às infrações referidas no artigo 2.º.

Artigo 6.º Sanções
1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infrações referidas nos artigos 2.o, 3.o, 4.o e 5.o sejam passíveis de sanções penais efetivas, proporcionadas e dissuasivas.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infrações referidas nos artigos 3.º e 4.º sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, um a três anos.

Artigo 7.º Circunstâncias agravantes

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que a infração referida no n.º 2 do artigo 2.o e as referidas nos artigos 3.o e 4.o sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, dois a cinco anos quando forem praticadas no âmbito de uma organização criminosa, tal como definida na Ação Comum 98/733/JAI, independentemente do nível da pena nesta referido.

2. Um Estado-Membro pode também tomar as medidas a que se refere o n.º 1 nos casos em que a infração em causa tenha causado danos graves ou lesado interesses essenciais.

Artigo 8.º Responsabilidade das pessoas coletivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser consideradas responsáveis pelas infrações referidas nos artigos 2.º, 3.º, 4.º e 5.º, praticadas em seu benefício por qualquer pessoa, agindo individualmente ou enquanto integrando um órgão da pessoa coletiva, que nela ocupe uma posição dominante baseada:

a) Nos seus poderes de representação da pessoa coletiva; ou

b) No seu poder para tomar decisões em nome da pessoa coletiva; ou

c) Na sua autoridade para exercer controlo dentro da pessoa coletiva.

2. Para além dos casos previstos no n.º 1, os Estados-Membros devem assegurar que uma pessoa coletiva possa ser considerada responsável sempre que a falta de vigilância ou de controlo por parte de uma pessoa referida no n.º 1 tenha tornado possível a prática, por uma pessoa que lhe esteja subordinada, das infrações referidas nos artigos 2.o, 3.o, 4.o e 5.o, em benefício dessa pessoa coletiva.

3. A responsabilidade de uma pessoa coletiva nos termos dos n.ºs 1 e 2 não exclui a instauração de procedimento penal contra as pessoas singulares envolvidas na qualidade de autoras, instigadoras ou cúmplices nas infrações referidas nos artigos 2.º, 3.º, 4.º e 5.º.

Artigo 9.º Sanções aplicáveis às pessoas coletivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do n.º 1 do artigo 8.o seja passível de sanções efetivas, proporcionadas e dissuasivas, incluindo multas ou coimas e eventualmente outras sanções, designadamente:

a) Exclusão do benefício de vantagens ou auxílios públicos;

b) Interdição temporária ou permanente de exercer atividade comercial;

c) Colocação sob vigilância judicial;

d) Dissolução por via judicial.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do n.º 2 do artigo 8.º seja passível de sanções ou medidas efetivas, proporcionadas e dissuasivas.

Artigo 10.º Competência

1. Cada Estado-Membro deve definir a sua competência relativamente às infrações referidas nos artigos 2.o, 3.o, 4.o e 5.o, sempre que a infração tiver sido praticada:

a) Total ou parcialmente no seu território; ou

b) Por um nacional seu; ou

c) Em benefício de uma pessoa coletiva com sede no seu território.

2. Ao definir a sua competência em conformidade com a alínea a) do n.º 1, cada Estado-Membro deve assegurar que sejam incluídos os casos em que:

a) O autor praticou a infração quando se encontrava fisicamente presente no território desse Estado-Membro, independentemente de a infração visar ou não um sistema de informação situado no seu território; ou

b) A infração foi praticada contra um sistema de informação situado no território desse Estado-Membro, independentemente de o autor da infração se encontrar ou não fisicamente presente no seu território.

3. Qualquer Estado-Membro que, nos termos do seu direito, ainda não extradite ou entregue os seus nacionais, deve tomar as medidas necessárias para definir a sua competência e, eventualmente, para instaurar procedimento penal relativamente às infrações referidas nos artigos 2.º, 3.º, 4.º e 5.º, quando praticadas por um dos seus nacionais fora do seu território.

4. Sempre que uma infração seja da competência de mais do que um Estado-Membro e qualquer um deles possa validamente instaurar procedimento penal com base nos mesmos factos, os Estados-Membros em causa devem cooperar para decidir qual deles moverá o procedimento contra os autores da infração, tendo em vista centralizá-lo, se possível, num único Estado-Membro. Para o efeito, os Estados-Membros podem recorrer a qualquer órgão ou mecanismo instituído no seio da União Europeia para facilitar a cooperação entre as suas autoridades judiciais e a coordenação das respetivas ações. Serão tidos em conta, sucessivamente, os seguintes elementos:
- o Estado-Membro ser aquele em cujo território foram praticadas as infrações, nos termos da alínea a) do n.º 1 e do n.º 2,
- o Estado-Membro ser o da nacionalidade do autor,
- o Estado-Membro ser aquele em cujo território o autor foi encontrado.

5. Qualquer Estado-Membro pode decidir que não aplicará ou que só aplicará em casos ou condições específicos, as regras de competência estabelecidas nas alíneas b) e c) do n.º 1.

6. Sempre que decidirem aplicar o n.º 5, os Estados-Membros devem informar desse facto o Secretariado-Geral do Conselho e a Comissão, indicando, se necessário, os casos ou condições especiais em que a decisão se aplica.

Artigo 11.º Intercâmbio de informações
1. Para efeitos da troca de informações relativa às infrações referidas

nos artigos 2.º, 3.º, 4.º. e 5.º e de acordo com as normas em matéria de proteção de dados, os Estados-Membros devem recorrer à rede existente de pontos de contacto operacionais, disponíveis 24 horas por dia e sete dias por semana.

2. Cada Estado-Membro deve notificar ao Secretariado-Geral do Conselho e à Comissão o ponto de contacto designado para efeitos de troca de informações sobre infrações relacionadas com ataques contra sistemas de informação. O Secretariado-Geral transmite essa informação aos restantes Estados-Membros.

Artigo 12.º Transposição

1. Os Estados-Membros devem tomar as medidas necessárias para dar cumprimento às disposições da presente decisão-quadro até 16 de Março de 2007.

2. Os Estados-Membros devem transmitir ao Secretariado-Geral do Conselho e à Comissão, até 16 de Março de 2007, o texto das disposições que transpõem para o respetivo direito nacional as obrigações resultantes da presente decisão-quadro. Até 16 de Setembro de 2007, com base num relatório elaborado a partir daquelas informações e num relatório escrito apresentado pela Comissão, o Conselho verifica em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente decisão-quadro.

Artigo 13.º Entrada em vigor

A presente decisão-quadro entra em vigor na data da sua publicação no Jornal Oficial da União Europeia.

Feito em Bruxelas, em 24 de Fevereiro de 2005.
Pelo Conselho
O Presidente
N. SCHMIT

19. Diretiva 2013/40/UE
do Parlamento Europeu e do Conselho
de 12 de agosto de 2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 83.º, n.º 1,

Tendo em conta a proposta da Comissão Europeia, Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[91],

Deliberando de acordo com o processo legislativo ordinário[92],

Considerando o seguinte:

1 // A presente diretiva tem como objetivos aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes, nomeadamente a polícia e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei, bem como as agências e organismos especializados competentes da União, tais como a Eurojust, a Europol e o seu Centro Europeu de Cibercriminalidade, e a Agência Europeia para a Segurança das Redes e da Informação (ENISA).

2 // Os sistemas de informação são um elemento essencial para a interação política, social e económica na União. A sociedade está muito e cada vez mais dependente deste tipo de sistemas. O bom funcionamento e a segurança desses sistemas na União são vitais para o desenvolvimento do mercado interno e de uma economia competitiva e inovadora.

---

[91] JO C 218 de 23.7.2011, p. 130.

[92] Posição do Parlamento Europeu de 4 de julho de 2013 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 22 de julho de 2013.

Assegurar um nível adequado de proteção dos sistemas de informação deverá ser parte integrante de um quadro eficaz e exaustivo de medidas de prevenção que acompanhe as respostas do direito penal à cibercriminalidade.

3 // Os ataques contra os sistemas de informação e, em especial, os ataques ligados à criminalidade organizada constituem uma ameaça crescente a nível da União e a nível mundial, e a eventualidade de ataques terroristas ou de natureza política contra os sistemas de informação que fazem parte da infraestrutura crítica dos Estados-Membros e da União suscita uma preocupação cada vez maior. Esta ameaça pode pôr em causa a realização de uma sociedade da informação mais segura e de um espaço de liberdade, segurança e justiça e, por conseguinte, exige uma resposta ao nível da União e cooperação e coordenação reforçadas a nível internacional.

4 // Existem na União diversas infraestruturas críticas cuja perturbação ou destruição teria um impacto transfronteiriço significativo. A necessidade de aumentar a capacidade de proteger a infraestrutura crítica da União tornou claro que as medidas contra os ciberataques deverão ser complementadas por sanções penais estritas que reflitam a gravidade desses ataques. A infraestrutura crítica pode ser entendida como um conjunto de elementos, sistemas ou partes destes situados nos Estados-Membros, essenciais para a manutenção das funções societais vitais, da saúde, da segurança e do bem-estar económico e social das pessoas, como centrais energéticas, redes de transportes ou redes governamentais, cuja perturbação ou destruição teria um impacto significativo num Estado-Membro devido à impossibilidade de continuar a assegurar tais funções.

5 // Existem provas de uma tendência para perpetrar ciberataques cada vez mais perigosos e recorrentes em larga escala contra sistemas de informação que podem frequentemente ser cruciais para os Estados-Membros ou para certas funções específicas do setor público ou privado. Esta tendência é acompanhada pelo desenvolvimento de métodos cada vez mais sofisticados, como a criação e utilização das chamadas «botnets», que implicam várias fases de um ato criminoso, cada uma das quais podendo constituir por si só um grave risco para o interesse público. A presente diretiva visa, nomeadamente,

introduzir sanções penais para a criação de «botnets», a saber, o ato de estabelecer o controlo à distância de grande número de computadores mediante a respetiva contaminação com software maligno através de ciberataques focalizados. Uma vez criada, a rede de computadores infetados que constituem a «botnet» pode ser ativada sem o conhecimento dos utilizadores dos computadores a fim de lançar um ciberataque em grande escala, o que geralmente tem o potencial de provocar danos graves, como se refere na presente diretiva. Os Estados-Membros podem determinar o que constitui um dano grave nos termos do seu direito e da sua prática nacionais, como, por exemplo, a perturbação de serviços de sistema de importância pública significativa, ou importantes custos financeiros ou a perda de dados pessoais ou informações sensíveis.

6 // Os ciberataques em larga escala podem provocar prejuízos económicos substanciais, quer através da interrupção de sistemas de informação e comunicação, quer através da perda ou alteração de informações comerciais confidenciais importantes ou de outros dados. Deverá ser prestada especial atenção à sensibilização das pequenas e médias empresas inovadoras para as ameaças decorrentes destes ataques e para a sua vulnerabilidade aos mesmos, visto que essas empresas dependem cada vez mais do bom funcionamento e da disponibilidade de sistemas de informação, e dispõem frequentemente de recursos limitados no domínio da segurança da informação.

7 // É necessário adotar uma abordagem comum dos elementos constitutivos das infrações penais, introduzindo como infrações comuns o acesso ilegal aos sistemas de informação, a interferência ilegal em sistemas, a interferência ilegal nos dados e a interceção ilegal.

8 // A interceção compreende, embora não necessariamente de forma exclusiva, a escuta, monitorização ou vigilância do conteúdo de comunicações e a obtenção do conteúdo de dados, quer diretamente, por meio do acesso e utilização dos sistemas de informação, quer indiretamente, através da utilização de dispositivos eletrónicos de escuta não autorizada ou de escuta por meios técnicos.

9 // Os Estados-Membros deverão prever sanções para os ataques contra os sistemas de informação. Essas sanções deverão ser efetivas,

proporcionadas e dissuasivas, e deverão incluir penas de prisão e/ou sanções pecuniárias.

10 // A presente diretiva prevê sanções penais pelo menos para os casos que se revestem de alguma gravidade. Os Estados-Membros podem determinar o que constitui um caso de pouca gravidade de acordo com o seu direito e a sua prática nacionais. Pode, por exemplo, considerar-se de pouca gravidade uma infração cujos danos ou risco para os interesses públicos ou privados, como a integridade de um sistema informático ou de dados informáticos, ou a integridade, os direitos ou outros interesses de uma pessoa, sejam insignificantes ou de natureza tal que tornem desnecessária a imposição quer de sanções penais dentro dos limites legais quer de responsabilidade criminal.

11 // A identificação e comunicação das ameaças e dos riscos que representam os ciberataques e da correspondente vulnerabilidade dos sistemas de informação constituem um elemento importante para prevenir e responder com eficácia aos ciberataques e para melhorar a segurança dos sistemas de informação. A concessão de incentivos à comunicação das falhas de segurança poderá contribuir para esse efeito. Os Estados-Membros deverão procurar oferecer oportunidades para a deteção e a comunicação legais das falhas de segurança.

12 // Convém prever sanções mais severas para os casos em que os ataques contra um sistema de informação sejam perpetrados por organizações criminosas, na aceção da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada[93], ou em que os ciberataques sejam realizados em larga escala, afetando deste modo um número significativo de sistemas de informação, nomeadamente quando visam criar uma «botnet», ou quando causam danos graves, incluindo quando são perpetrados através de uma «botnet». Deverão igualmente prever-se sanções mais severas caso os ataques sejam dirigidos contra infraestruturas críticas dos Estados-Membros ou da União.

13 // A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento

[93] *JO L 300 de 11.11.2008, p. 42.*

importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União.

14 // Nas suas conclusões de 27 e 28 de novembro de 2008, o Conselho indicou que deveria ser desenvolvida pelos Estados-Membros e pela Comissão uma nova estratégia, tendo em conta o conteúdo da Convenção do Conselho da Europa sobre a Criminalidade Informática de 2001. Essa Convenção constitui o enquadramento legal de referência do combate à cibercriminalidade, incluindo os ataques contra os sistemas de informação. A presente diretiva baseia-se nessa Convenção. A conclusão do processo de ratificação dessa Convenção por todos os Estados-Membros o mais rapidamente possível deverá ser considerada prioritária.

15 // Tendo em conta as diferentes formas como os ataques podem ser realizados e a rápida evolução do hardware e do software, a presente diretiva faz referência a instrumentos que podem ser utilizados para cometer as infrações nela previstas. Esses instrumentos podem abranger o software maligno, incluindo o software capaz de criar «botnets», utilizado para cometer ciberataques. Mesmo que um desses instrumentos seja adequado ou especialmente adequado para cometer uma das infrações previstas na presente diretiva, pode perfeitamente ter sido produzido para um fim legítimo. Atendendo à necessidade de evitar a criminalização nos casos em que tais instrumentos sejam produzidos e colocados no mercado para fins legítimos, tais como testar a fiabilidade de produtos das tecnologias da informação ou a segurança de sistemas de informação, deverá estar preenchido, além do requisito geral de intenção, o requisito da intenção direta de utilizar esses instrumentos para cometer pelo menos uma das infrações previstas na presente diretiva.

16 // A presente diretiva não imputa responsabilidade penal nos casos em que, embora estando preenchidos os critérios objetivos que configuram as infrações nela previstas, os atos sejam cometidos sem intenção criminosa, por exemplo caso uma pessoa ignore que o acesso não era autorizado ou caso o agente esteja mandatado para testar ou proteger sistemas de informação, nomeadamente quando é

incumbido por uma empresa ou por um vendedor de testar a solidez do seu sistema de segurança. No contexto da presente diretiva, as obrigações contratuais ou os acordos de restrição de acesso a sistemas de informação por via da política de utilizadores ou das condições de serviço, ou os litígios laborais relativos ao acesso aos sistemas de informação do empregador e respetiva utilização para fins privados, não deverão implicar responsabilidade penal quando o acesso nessas circunstâncias seja considerado não autorizado e constitua portanto a única base para a ação penal. A presente diretiva não prejudica o direito de acesso à informação consagrado na legislação nacional e da União, mas também não pode servir de justificação para um acesso ilegal ou arbitrário à informação.

17 // A prática dos ciberataques poderá ser facilitada por várias circunstâncias, por exemplo nos casos em que o autor da infração tenha acesso a sistemas de segurança inerentes aos sistemas de informação afetados no âmbito do seu emprego. No contexto do direito nacional, essas circunstâncias deverão ser devidamente tidas em conta, se for caso disso, no desenrolar dos processos penais.

18 // Os Estados-Membros deverão prever no seu direito nacional circunstâncias agravantes conformes com as regras do seu ordenamento jurídico aplicáveis na matéria. Deverão assegurar que tais circunstâncias agravantes possam ser consideradas pelos juízes ao proferirem a sentença. A apreciação dessas circunstâncias é deixada ao livre arbítrio do juiz, a par dos outros elementos factuais de cada caso.

19 // A presente diretiva não regula as condições do exercício da competência relativamente a qualquer das infrações nela referidas, como sejam a existência de um relato da vítima feito no local da prática da infração ou de uma denúncia por parte do Estado no qual a infração tenha sido cometida, ou ainda o facto de o autor da infração não ter sido sujeito a ação penal no local em que a infração foi cometida.

20 // No contexto da presente diretiva, os Estados e os organismos públicos continuam a estar plenamente obrigados a garantir o respeito dos direitos humanos e das liberdades fundamentais, em conformidade com as obrigações internacionais vigentes.

21 // A presente diretiva reforça a importância das redes, como a rede do G8 ou a rede de pontos de contacto do Conselho da Europa disponíveis 24 horas por dia e sete dias por semana. Estes pontos de contacto deverão poder prestar uma assistência efetiva, facilitando, por exemplo, a troca das informações relevantes disponíveis e a prestação de aconselhamento técnico ou de informações jurídicas para efeito de inquéritos ou procedimentos relativos a infrações penais relacionadas com sistemas de informação e dados conexos que digam respeito ao Estado-Membro requerente. Para assegurar o bom funcionamento das redes, cada ponto de contacto deverá ter a capacidade de efetuar comunicações urgentes com os pontos de contacto dos outros Estados-Membros, nomeadamente com o apoio de pessoal formado e equipado. Dada a velocidade com que os ciberataques em larga escala podem ser realizados, os Estados-Membros deverão poder responder prontamente aos pedidos urgentes provenientes desta rede de pontos de contacto. Em tais casos, pode ser oportuno que o pedido de informação seja acompanhado de um contacto telefónico, a fim de assegurar o tratamento rápido do pedido pelo Estado-Membro requerido e a transmissão de uma resposta no prazo de oito horas.

22 // A cooperação entre as autoridades públicas, por um lado, e o setor privado e a sociedade civil, por outro, é de grande importância para evitar e combater os ataques contra os sistemas de informação. É necessário promover e melhorar a cooperação entre os prestadores de serviços, os produtores, os organismos responsáveis pela aplicação da lei e as autoridades judiciais, respeitando plenamente o Estado de direito. Essa cooperação poderá incluir, por exemplo, o apoio dos prestadores de serviços na preservação de eventuais provas, no fornecimento de elementos que ajudem a identificar os autores de infrações e, em última instância, no encerramento total ou parcial, nos termos do direito e da prática nacionais, de sistemas de informação ou de funções comprometidos ou utilizados para fins ilegais. Os Estados-Membros deverão também considerar a possibilidade de criar redes de cooperação e de parceria com os prestadores de serviços e com os produtores para a troca de informações relacionadas com as infrações que recaiam no âmbito de aplicação da presente diretiva.

23 // É necessário recolher dados comparáveis sobre as infrações previstas na presente diretiva. Os dados relevantes deverão ser postos

à disposição das agências e organismos especializados competentes da União, como a Europol e a ENISA, em função das respetivas atribuições e necessidades de informação, a fim de obter uma imagem mais completa do problema da cibercriminalidade e da segurança das redes e da informação a nível da União e contribuindo, desse modo, para a formulação de uma resposta mais eficaz. Os Estados-Membros deverão transmitir à Europol e ao seu Centro Europeu de Cibercriminalidade informações sobre o modus operandi dos infratores, para efeitos da realização de avaliações de ameaça e de análises estratégicas da cibercriminalidade, nos termos da Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia (Europol)[94]. A prestação de informações pode facilitar uma melhor compreensão das ameaças atuais e futuras e contribuir assim para a tomada de decisões mais adequadas e focalizadas sobre o combate e a prevenção dos ataques contra os sistemas de informação.

24 // A Comissão deverá apresentar um relatório sobre a aplicação da presente diretiva e fazer as propostas legislativas necessárias, suscetíveis de conduzir a um alargamento do seu âmbito, tendo em conta a evolução no domínio da cibercriminalidade. Tal evolução pode incluir avanços tecnológicos diversos, nomeadamente os que permitam uma aplicação mais eficaz da legislação relativa a ataques contra sistemas de informação, ou que facilitem a prevenção ou minimizem o impacto de tais ataques. Para esse efeito, a Comissão deverá ter em conta as análises e os relatórios disponíveis elaborados pelos intervenientes relevantes, em particular a Europol e a ENISA.

25 // A fim de combater eficazmente a cibercriminalidade, é necessário aumentar a resiliência dos sistemas de informação, tomando as medidas adequadas para os proteger de forma mais eficaz contra os ciberataques. Os Estados-Membros deverão tomar as medidas necessárias para proteger as suas infraestruturas críticas contra os ciberataques, contexto em que deverão considerar a proteção dos seus sistemas de informação e dos dados a eles associados. A garantia de um nível adequado de proteção e segurança dos sistemas de informação pelas pessoas coletivas, por exemplo, no âmbito da prestação de serviços de comunicações eletrónicas publicamente disponíveis nos termos

[94] *JO L 121 de 15.5.2009, p. 37.*

da legislação da União em vigor no domínio da privacidade e da proteção das comunicações e dos dados eletrónicos, constitui uma parte essencial de uma abordagem abrangente de luta eficaz contra a cibercriminalidade. Deverão ser assegurados níveis de proteção adequados contra ameaças e vulnerabilidades razoavelmente identificáveis, de acordo com os conhecimentos técnicos e tecnológicos disponíveis em setores específicos e tendo em conta as situações concretas de cada um em matéria de tratamento de dados. Os custos e os encargos inerentes a essa proteção deverão ser proporcionais aos danos que um ciberataque poderia causar às pessoas afetadas. Os Estados-Membros são incentivados a prever, no contexto do seu direito nacional, as medidas necessárias para responsabilizar as pessoas coletivas que manifestamente não assegurem um nível adequado de proteção contra ciberataques.

26 // As consideráveis lacunas e diferenças entre as legislações e os procedimentos penais dos Estados-Membros no domínio dos ataques contra os sistemas de informação podem entravar a luta contra a criminalidade organizada e o terrorismo e dificultar uma cooperação policial e judiciária efetiva nesta área. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas tenham uma dimensão transfronteiriça, o que evidencia a necessidade urgente de adotar medidas suplementares para aproximar o direito penal neste domínio. Além disso, a coordenação da ação penal contra casos de ataques a sistemas de informação deverá ser facilitada pela transposição e aplicação adequadas da Decisão-Quadro 2009/948/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal[95]. Os Estados-Membros deverão também, em cooperação com a União, procurar melhorar a cooperação internacional relacionada com a segurança dos sistemas de informação e das redes e dados informáticos. Deverá ser devidamente tida em conta a segurança da transferência e do armazenamento de dados em todos os acordos internacionais que impliquem o intercâmbio de dados.

27 // É essencial uma melhor cooperação entre os organismos responsáveis pela aplicação da lei e as autoridades judiciais da União para um combate eficaz contra a cibercriminalidade. Neste contexto, deverá

[95] *JO L 328 de 15.12.2009, p. 42.*

ser incentivada a intensificação dos esforços para facultar às autoridades relevantes uma formação adequada para aumentar a compreensão da cibercriminalidade e do seu impacto e para promover a cooperação e o intercâmbio de melhores práticas, por exemplo, através das agências e organismos especializados competentes da União. Essa formação deverá ter por objetivo, nomeadamente, uma maior sensibilização para os diferentes sistemas jurídicos nacionais, os eventuais desafios jurídicos e técnicos que se colocam nas investigações criminais e a partilha de competências entre as autoridades nacionais competentes.

28 // A presente diretiva respeita os direitos humanos e as liberdades fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, designadamente a proteção dos dados pessoais, o respeito da vida privada, a liberdade de expressão e de informação, o direito a um tribunal imparcial, a presunção de inocência e os direitos de defesa, bem como os princípios da legalidade e da proporcionalidade dos delitos e das penas. Em particular, a presente diretiva procura garantir o pleno respeito desses direitos e princípios, pelo que deve ser aplicada em conformidade.

29 // A proteção dos dados pessoais é um direito fundamental consagrado pelo artigo 16.º, n.º 1, do TFUE e pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. Por conseguinte, o tratamento de dados pessoais no quadro da aplicação da presente diretiva deverá ser plenamente conforme com a legislação da União aplicável à proteção de dados.

30 // Nos termos do artigo 3.o do Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, estes Estados-Membros notificaram por escrito a sua intenção de participar na adoção e aplicação da presente diretiva.

31 // Nos termos dos artigos 1.o e 2.o do Protocolo relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adoção da presente diretiva e não fica a ela vinculada nem sujeita à sua aplicação.

32 // Atendendo a que os objetivos da presente diretiva, a saber, sujeitar os ataques contra os sistemas de informação, em todos os Estados-Membros, a sanções penais efetivas, proporcionadas e dissuasivas e melhorar e incentivar a cooperação entre autoridades judiciais e outras autoridades competentes, não podem ser suficientemente realizados pelos Estados-Membros, e podem, pois, devido à sua dimensão e efeitos, ser mais bem alcançados ao nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade, consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir esses objetivos.

33 // A presente diretiva visa alterar e alargar o âmbito das disposições da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação[96]. Dado que as alterações a introduzir são numerosas e substanciais, a Decisão-Quadro 2005/222/JAI deverá, por uma questão de clareza, ser integralmente substituída no que se refere aos Estados-Membros que participam na adoção da presente diretiva,

ADOTARAM A PRESENTE DIRETIVA:

Artigo 1.º Objeto
A presente diretiva estabelece regras mínimas relativas à definição das infrações penais e das sanções no domínio dos ataques contra os sistemas de informação. Tem igualmente por objetivo facilitar a prevenção da prática desse tipo de infrações e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes.

Artigo 2.º Definições
Para efeitos da presente diretiva, entende-se por:
a) «Sistema de informação», um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

[96] *JO L 69 de 16.3.2005, p. 67.*

b) «Dados informáticos», uma representação de factos, informações ou conceitos de forma adequada para o tratamento num sistema de informação, incluindo um programa que permite que um sistema de informação execute uma dada função;

c) «Pessoa coletiva», uma entidade que beneficie do estatuto de pessoa coletiva por força do direito aplicável, excluindo Estados ou organismos públicos no exercício das suas prerrogativas de autoridade pública, e organizações internacionais de direito público;

d) «Não autorizado», um comportamento a que refere a presente diretiva, incluindo o acesso, a interferência ou a interceção, não consentido pelo proprietário ou por outro titular dos direitos do sistema ou de parte dele, ou não permitido pelo direito nacional.

Artigo 3.º Acesso ilegal a sistemas de informação
Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional e não autorizado à totalidade ou a parte de um sistema de informação seja punível como infração penal caso a infração seja cometida mediante a violação de uma medida de segurança, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 4.º Interferência ilegal no sistema
Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo dados informáticos, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo esses dados, ou tornando-os inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 5.º Interferência ilegal nos dados
Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de apagar, danificar, deteriorar, alterar ou suprimir dados informáticos de um sistema de informação, ou de os tornar inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 6.º Interceção ilegal
Os Estados-Membros devem tomar as medidas necessárias para assegurar que a interceção intencional e não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos para, a partir de ou num sistema de informação, incluindo emissões eletromagnéticas de um sistema de informação que comporte esses dados, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 7.º Instrumentos utilizados para cometer infrações
Os Estados-Membros devem tomar as medidas necessárias para assegurar que a produção, venda, aquisição para utilização, importação, distribuição ou qualquer outra forma de disponibilização de um dos seguintes instrumentos, não autorizadas e com o intuito da sua utilização para a prática de uma das infrações previstas nos artigos 3.o a 6.o, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade:
a) Um programa informático, concebido ou adaptado essencialmente para cometer uma das infrações previstas nos artigos 3.º a 6.º;

b) Uma senha, um código de acesso ou dados similares que permitam aceder à totalidade ou a parte de um sistema de informação.

Artigo 8.º Instigação, cumplicidade e tentativa
1. Os Estados-Membros devem assegurar que a instigação e a cumplicidade na prática de uma infração prevista nos artigos 3.º a 7.º sejam puníveis como infrações penais.

2. Os Estados-Membros devem assegurar que a tentativa da prática de uma das infrações previstas nos artigos 4.º e 5.º seja punível como infração penal.

Artigo 9.º Sanções
1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 8.º sejam puníveis com sanções penais efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 7.º sejam puníveis

com uma pena máxima de prisão não inferior a dois anos, pelo menos nos casos que se revistam de alguma gravidade.

3. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 4.º e 5.º, caso sejam cometidas intencionalmente e afetem um número significativo de sistemas de informação recorrendo a um dos instrumentos referidos no artigo 7.º, concebido ou adaptado essencialmente para esse fim, sejam puníveis com uma pena máxima de prisão não inferior a três anos.

4. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 4.º e 5.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos caso:
a) Sejam cometidas no âmbito de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção nela prevista;

b) Causem danos graves; ou

c) Sejam cometidas contra um sistema de informação que constitua uma infraestrutura crítica.

5. Os Estados-Membros devem tomar as medidas necessárias para assegurar que, caso as infrações previstas nos artigos 4.º e 5.º sejam cometidas mediante a utilização abusiva de dados pessoais de outra pessoa com o objetivo de conquistar a confiança de terceiros, causando assim danos ao legítimo titular da identidade, tal possa, de acordo com o direito nacional, ser considerado uma circunstância agravante, salvo se tal circunstância já estiver abrangida por outra infração punível pelo direito nacional.

Artigo 10.º Responsabilidade das pessoas coletivas
1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser consideradas responsáveis pelas infrações previstas nos artigos 3.o a 8.o, cometidas em seu benefício por qualquer pessoa, agindo a título individual ou enquanto membro de um dos seus órgãos e que nela tenha uma posição dirigente, com base num dos seguintes elementos:
a) Poder de representação da pessoa coletiva;

b) Poderes para tomar decisões em nome da pessoa coletiva;

c) Poderes para exercer controlo dentro da pessoa coletiva.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser consideradas responsáveis caso a falta de supervisão ou de controlo por parte de uma das pessoas referidas no n.º 1 tenha tornado possível a prática, por uma pessoa sob a sua autoridade, de uma das infrações previstas nos artigos 3.º a 8.º em benefício dessa pessoa coletiva.
3. A responsabilidade das pessoas coletivas por força dos n.ºs 1 e 2 não exclui a ação penal contra as pessoas singulares que sejam autoras, instigadoras ou cúmplices de uma das infrações previstas nos artigos 3.º a 8.º .

Artigo 11.º Sanções aplicáveis às pessoas coletivas
1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do artigo 10.º, n.º 1, seja passível de sanções efetivas, proporcionadas e dissuasivas, incluindo multas ou coimas e, nomeadamente:
a) A exclusão do direito a benefícios ou auxílios públicos;

b) A proibição temporária ou permanente de exercer atividades comerciais;

c) A colocação sob vigilância judicial;

d) A liquidação judicial;

e) O encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática da infração.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do artigo 10.º, n.º 2, seja passível de sanções ou de outras medidas efetivas, proporcionadas e dissuasivas.

Artigo 12.º Competência
1. Os Estados-Membros devem determinar a sua própria competência relativamente às infrações previstas nos artigos 3.º a 8.º caso a infração tenha sido cometida:

a) Total ou parcialmente no seu território; ou

b) Por um dos seus nacionais, pelo menos nos casos em que o ato constitua infração no local em que seja praticado.

2. Ao determinarem a sua competência nos termos do n.º 1, alínea a), os Estados-Membros devem assegurar que são competentes nos casos em que:
a) O autor tenha cometido a infração quando se encontrava fisicamente presente no seu território, independentemente de a infração ter ou não sido cometida contra um sistema de informação situado nesse território; ou

b) A infração tenha sido cometida contra um sistema de informação situado no seu território, independentemente de o seu autor se encontrar ou não fisicamente presente nesse território;

3. Os Estados-Membros devem informar a Comissão caso decidam alargar a sua competência às infrações previstas nos artigos 3.º a 8.º cometidas fora do seu território, nomeadamente caso:
a) O autor tenha a sua residência habitual no seu território; ou

b) A infração tenha sido cometida em benefício de uma pessoa coletiva estabelecida no seu território.

Artigo 13.º Troca de informações
1. Para efeitos da troca de informações relativas às infrações previstas nos artigos 3.º a 8.º, os Estados-Membros devem assegurar a existência de um ponto de contacto operacional nacional e recorrer à rede existente de pontos de contacto operacionais disponível 24 horas por dia e sete dias por semana. Os Estados-Membros devem também assegurar a existência de procedimentos que, em caso de pedidos de assistência urgentes, lhes permitam indicar, no prazo máximo de oito horas a contar da receção do pedido, se o pedido de ajuda será deferido, e a forma e o prazo estimado de resposta.

2. Os Estados-Membros devem informar a Comissão do seu ponto de contacto referido no n.º 1. A Comissão deve transmitir essa informação aos restantes Estados-Membros e às agências e órgãos especializados competentes da União.

3. Os Estados-Membros devem tomar as medidas necessárias para assegurar a disponibilização de canais de comunicação adequados para facilitar a comunicação sem atrasos indevidos das infrações previstas nos artigos 3.o a 6.o às autoridades nacionais competentes.

Artigo 14.º Acompanhamento e estatísticas
1. Os Estados-Membros devem assegurar a criação de um sistema de registo, produção e disponibilização de dados estatísticos sobre as infrações previstas nos artigos 3.º a 7.º.

2. As estatísticas referidas no n.º 1 devem abranger, no mínimo, os dados existentes sobre o número de infrações previstas nos artigos 3.º a 7.º registadas pelos Estados-Membros, e sobre o número de pessoas alvo de ação penal e condenadas pelas infrações previstas nos artigos 3.º a 7.º.

3. Os Estados-Membros devem transmitir à Comissão os dados recolhidos nos termos do presente artigo. A Comissão deve assegurar a publicação de uma revisão consolidada destes relatórios estatísticos e a sua transmissão às agências e organismos especializados competentes da União.

Artigo 15.º Substituição da Decisão-Quadro 2005/222/JAI
A Decisão-Quadro 2005/222/JAI é substituída, no que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, sem prejuízo das obrigações dos Estados-Membros quanto ao prazo de transposição daquela decisão-quadro para o direito nacional.
No que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, as remissões para a Decisão-Quadro 2005/222/JAI devem entender-se como sendo feitas para a presente diretiva.

Artigo 16.º Transposição
1. Os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 4 de setembro de 2015.

2. Os Estados-Membros comunicam à Comissão o texto das disposições que transpõem para o respetivo direito interno as obrigações que sobre eles impendem por força da presente diretiva.

3. Quando os Estados-Membros adotarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa referência são estabelecidas pelos Estados-Membros.

Artigo 17.º Relatórios
Até 4 de setembro de 2017, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório no qual avalie em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente diretiva, acompanhado, se necessário, de propostas legislativas. A Comissão deve também ter em conta o progresso técnico e jurídico em matéria de cibercriminalidade, particularmente no que respeita ao âmbito de aplicação da presente diretiva.

Artigo 18.º Entrada em vigor
A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

Artigo 19.º Destinatários
Os destinatários da presente diretiva são os Estados-Membros, nos termos dos Tratados.

Feito em Bruxelas, em 12 de agosto de 2013.

Pelo Parlamento Europeu

O Presidente
M. SCHULZ

Pelo Conselho
O Presidente
L. LINKEVIČIUS

20. Decreto-lei nº 134/2009, de 2 de Junho, estabelece o regime jurídico aplicável à prestação de serviços de promoção, informação e apoio aos consumidores e utentes através de centros telefónicos de relacionamento (call centers)[97]

No mercado atual, o relacionamento entre o consumidor e a empresa é cada vez menos presencial, tendo vindo a assistir-se a uma aposta na prestação de serviços de apoio ao cliente através de centros telefónicos de relacionamento (call centers), com benefícios para as empresas mas também para os consumidores, que obtêm de forma mais cómoda a informação e o apoio de que necessitam. No entanto, a experiência demonstra que sendo o centro telefónico de relacionamento (call center) de uma empresa o ponto de contacto do consumidor, este tem, muitas vezes, dificuldade em obter o apoio e a informação a que tem direito ou em exercer direitos basilares e que querendo reclamar da deficiente prestação de informação não lhe são dados os meios adequados e necessários. Torna-se, assim, necessário salvaguardar o direito à informação por parte de consumidor, regulando a forma como esta é prestada e estabelecendo regras que contribuam para a eficiência do serviço. Das novas regras, destaca-se a proibição de fazer o consumidor esperar em linha mais de 60 s e, no caso de serviço de atendimento relativo a um serviço de execução continuada ou periódica, estabelece-se a obrigação de disponibilizar ao consumidor uma opção que lhe permita o cancelamento do serviço, que permita ao consumidor, consoante o caso, proceder ao cancelamento do serviço ou obter informação quanto aos procedimentos a adotar para tal.

É também fixado um conjunto de práticas proibidas, além de se estabelecerem regras sobre a divulgação dos números telefónicos utilizados para a prestação do serviço. De forma a respeitar o direito à privacidade do consumidor, a emissão de chamadas por parte dos profissionais passa a estar sujeita a um horário.

O presente decreto-lei aplica-se aos profissionais que, no âmbito de uma atividade económica que vise a obtenção de benefícios, coloquem à disposição do consumidor um centro telefónico de relacionamento (call center). Assim, o presente decreto-lei não é aplicável aos serviços informativos assegurados por entidades públicas, no âmbito de uma

[97] *Última modificação legislativa: Decreto-Lei n.º 72-a/2010, de 18 de Junho*

concessão, com exceção dos prestadores de serviços públicos essenciais, tal como definidos no artigo 1.º da Lei n.º 23/96, de 26 de Julho, que coloquem à disposição dos utentes um centro de relacionamento telefónico, independentemente da sua natureza pública ou privada.
Foi ouvida a Associação Nacional de Municípios Portugueses.
Foi promovida a audição ao Conselho Nacional do Consumo. Foram ouvidos, a título facultativo, a Federação Nacional das Cooperativas de Consumidores, a União Geral dos Consumidores e a Associação Portuguesa de Contat Centers.

Artigo 1.º Objeto
O presente decreto-lei estabelece o regime jurídico aplicável à prestação de serviços de promoção, informação e apoio aos consumidores e utentes, através de centros telefónicos de relacionamento (call centers).

Artigo 2.º Âmbito de aplicação
1. O presente decreto-lei aplica-se a todos os profissionais que coloquem à disposição do consumidor um centro telefónico de relacionamento (call center).

2. O presente decreto-lei aplica-se aos prestadores de serviços públicos essenciais que coloquem à disposição do utente um centro telefónico de relacionamento (call center), independentemente da sua natureza pública ou privada.

3. O presente decreto-lei não prejudica o disposto no Decreto-Lei n.º 143/2001, de 26 de Abril, alterado pelo Decreto-Lei n.º 82/2008, de 20 de Maio, nem o disposto no Decreto-Lei n.º 95/2006, de 29 de Maio.

Artigo 3.º Definições
Para efeitos do presente decreto-lei, considera-se:
a) «Centro telefónico de relacionamento (call center)» a estrutura organizada e dotada de tecnologia que permite a gestão de um elevado tráfego telefónico para contacto com consumidores ou utentes, no âmbito de uma atividade económica, destinado, designadamente, a responder às suas solicitações e a contactá-los, com vista à promoção de bens ou serviços ou à prestação de informação e apoio;

b) «Consumidor» aquele assim definido nos termos do n.º 1 do artigo 2.º da Lei n.º 24/96, de 31 de Julho;

c) «Profissional» qualquer pessoa singular ou coletiva que exerça com carácter profissional uma atividade económica que vise a obtenção de benefícios e coloque à disposição do consumidor um centro telefónico de relacionamento (call center);

d) «Serviços públicos essenciais» os serviços assim definidos nos termos do artigo 1.º da Lei n.º 23/96, de 26 de Julho, alterado pelas Leis n.os12/2008, de 26 de Fevereiro, e 24/2008, de 2 de Junho;

e) «Utente» aquele assim definido nos termos do n.º 3 do artigo 1.º da Lei n.º 23/96, de 26 de Julho, alterado pelas Leis n.ºs 12/2008, de 26 de Fevereiro, e 24/2008, de 2 de Junho;

f) «Prestador do serviço» aquele assim definido nos termos do n.º 4 do artigo 1.º da Lei n.º 23/96, de 26 de Julho, alterado pela Leis n.ºs 12/2008, de 26 de Fevereiro, e 24/2008, de 2 de Junho;

g) «Suporte durável» qualquer instrumento que permita ao consumidor armazenar informações de um modo permanente e acessível para referência futura e que não permita que as partes contratantes manipulem unilateralmente as informações armazenadas;

h) «Período de espera em linha» o período que medeia entre o atendimento pelo centro telefónico de relacionamento (call center) ou, existindo menu eletrónico, a escolha da opção de contacto com o profissional e o atendimento personalizado pelo profissional.

Artigo 4.º Regras gerais

1. O serviço do centro telefónico de relacionamento (call center) deve ser prestado através de um ou mais números de telefone exclusivos para acesso dos consumidores ou dos utentes e possuir os meios técnicos e humanos adequados ao cumprimento das suas funções.

2. O acesso ao serviço ou à informação não é condicionado ao prévio fornecimento de quaisquer dados pelo consumidor ou pelo utente,

sem prejuízo dos estritamente necessários para o tratamento da sua solicitação, bem como da garantia da confidencialidade da informação a prestar e da verificação da legitimidade do interlocutor para aceder à mesma.

3. O serviço do centro telefónico de relacionamento (call center) deve funcionar, pelo menos, num número de horas pré-estabelecido em período diurno e disponibilizar atendimento personalizado.

4. O atendimento só pode ser exclusivamente processado através de sistema de atendimento automático fora das horas de atendimento personalizado.

5. O número de telefone do serviço e o seu período do seu funcionamento, com destaque para o período de atendimento personalizado, devem constar, de forma bem visível, dos materiais de suporte de todas as comunicações do profissional.

Artigo 5.º Práticas proibidas

1. São proibidas as seguintes práticas:

a) O reencaminhamento da chamada para outros números que impliquem um custo adicional para o consumidor ou para o utente, salvo se, sendo devidamente informado do seu custo, o consumidor ou o utente expressamente o consentir;

b) A emissão de qualquer publicidade durante o período de espera no atendimento;

c) O registo em base de dados do número de telefone utilizado pelo consumidor ou pelo utente para efetuar a ligação telefónica, excecionadas as situações legalmente autorizadas.

2. No exercício da atividade abrangida pelo presente decreto-lei, o profissional deve abster-se de abusar da confiança, falta de experiência ou de conhecimentos do consumidor ou do utente ou aproveitar-se de qualquer estado de necessidade ou fragilidade em que o mesmo se encontre.

Artigo 6.º Atendimento

1. O atendimento é processado por ordem de entrada das chamadas, sem prejuízo da possibilidade de existência de menus eletrónicos e do disposto no n.º 5 do artigo 8.º

2. Uma vez atendida a chamada, o período de espera em linha não deve ser superior a 60 s.

3. Existindo menu eletrónico, este é disponibilizado imediatamente após o atendimento, contando-se o período de espera em linha previsto no número anterior a partir da escolha pelo consumidor ou pelo utente da opção de contacto com o profissional.

4. Caso não seja possível efetuar o atendimento no prazo referido no n.º 2, deve ser disponibilizada uma forma de o consumidor ou de o utente deixar o seu contacto e identificar a finalidade da chamada, devendo o profissional responder em prazo não superior a dois dias úteis.

5. Caso o serviço de atendimento disponibilize um menu eletrónico, este não pode conter mais de cinco opções iniciais, devendo uma destas ser a opção de contacto com o profissional, com exceção dos horários em que o atendimento se processe exclusivamente através de sistema de atendimento automático.

6. Tratando-se de um serviço de atendimento relativo a um serviço de execução continuada ou periódica, do menu referido no número anterior deve constar uma opção relativa ao cancelamento do serviço, que permita ao consumidor ou ao utente, consoante o caso, proceder ao cancelamento do serviço ou obter informação quanto aos procedimentos a adotar para tal.

7. Quando ocorra um pedido de cancelamento do serviço, o profissional deve enviar ao consumidor ou ao utente a confirmação do cancelamento, através de um suporte durável, no prazo máximo de três dias úteis.

8. Nos primeiros 90 dias contados da prestação do serviço, o ónus da prova do cumprimento das obrigações previstas no presente artigo cabe ao profissional.

Artigo 7.º Emissão de chamadas
1. As chamadas telefónicas dirigidas aos consumidores ou aos utentes devem ser efetuadas num horário que respeite os períodos de descanso em uso e nunca antes das 9 horas nem depois das 22 horas do fuso horário do consumidor ou dos utentes, salvo acordo prévio do mesmo.

2. O operador que efetue a chamada deve identificar-se imediatamente após o atendimento, bem como ao profissional em nome do qual atua e a finalidade do contacto.

3. Caso o consumidor ou o utente expresse a vontade de não prosseguir a chamada, esta deve ser desligada com urbanidade.

Artigo 8.º Prestação de informação
1. A prestação de informação obedece aos princípios da legalidade, boa-fé, transparência, eficiência, eficácia, celeridade e cordialidade.

2. A informação prestada aos consumidores ou aos utentes deve ser clara e objetiva, prestada em linguagem facilmente acessível, procurando satisfazer diretamente todas as questões colocadas.

3. Sem prejuízo da disponibilização de informação noutras línguas, as informações são prestadas em língua portuguesa.

4. As questões colocadas devem ser respondidas de imediato ou, não sendo possível, no prazo máximo de três dias úteis, contado da data da realização do contacto inicial pelo consumidor ou pelo utente, salvo motivo devidamente justificado.

5. Caso seja necessário, o serviço deve garantir a transferência para o sector competente para o atendimento definitivo da chamada, no tempo máximo de 60 s a contar do momento em que o operador verifica essa necessidade e desta dá conhecimento ao consumidor ou ao utente, sem prejuízo de o operador poder facultar ao consumidor ou ao utente o número direto de acesso ao mesmo.

6. A chamada não deve ser desligada pelo operador antes da conclusão do atendimento.

Artigo 9 Transparência
(Revogado)

Artigo 10.º Regime sancionatório
1. Constitui contraordenação o incumprimento do disposto no artigo 4.º, no n.º 1 do artigo 5.º, nos n.ºs 1 a 7 do artigo 6.º, nos n.ºs 1 e 2 do artigo 7.º e nos n.ºs 3 a 6 do artigo 8.º.

2. As contraordenações previstas no número anterior são puníveis com coima de € 250 até € 3740 ou de € 500 até € 44 890, consoante o infrator seja pessoa singular ou pessoa coletiva.

3. A negligência é sempre punível, sendo os limites máximos e mínimo reduzidos a metade.

Artigo 11.º Fiscalização e instrução dos processos de contraordenação
1. A fiscalização e a instrução dos processos de contraordenação competem ao regulador sectorial, competindo ao seu órgão máximo a aplicação das coimas e demais sanções.

2. A fiscalização e a instrução dos processos de contraordenação por violação do disposto no n.º 5 do artigo 4.º, quando cometidas através de publicidade, e na alínea b) do n.º 1 do artigo 5.º competem à Direcção-Geral do Consumidor, cabendo, neste caso, a aplicação de coimas e demais sanções à Comissão de Aplicação de Coimas em Matéria Económica e de Publicidade (CACMEP).

3. Nos restantes casos, a fiscalização e a instrução dos processos de contraordenação competem à Autoridade de Segurança Alimentar e Económica, cabendo, neste caso, a aplicação de coimas e demais sanções à CACMEP.

4. O produto das coimas previstas no presente artigo reverte em:
a) 60 % para o Estado;

b) 30 % para a entidade que instrui o processo de contraordenação;

c) 10 % para a entidade que aplica a coima, quando esta não coincida com a entidade que faz a instrução.

5. Caso coincidam na mesma entidade a instrução e a aplicação das coimas, a distribuição da receita é de 60% para o Estado e de 40 % para a entidade que instrui o processo.

Artigo 12.º Entrada em vigor
O presente decreto-lei entra em vigor 180 dias após a sua publicação.

Visto e aprovado em Conselho de Ministros de 11 de Março de 2009.
José Sócrates Carvalho Pinto de Sousa
Alberto Bernardes Costa
Fernando Pereira Serrasqueiro.

Promulgado em 20 de Maio de 2009.

Publique-se.

O Presidente da República,
Aníbal Cavaco Silva.

Referendado em 21 de Maio de 2009.
O Primeiro-Ministro,
José Sócrates Carvalho Pinto de Sousa.

21. Lei nº 6/99 de 27 de Janeiro, regula a publicidade domiciliária por telefone e por telecópia

Artigo 1.º Objeto e âmbito
1. A presente lei regula a publicidade domiciliária, nomeadamente por via postal, distribuição direta, telefone e telecópia.

2. A presente lei não se aplica à publicidade por correio eletrónico.

3. O regime fixado nas disposições seguintes não prejudica o disposto no artigo 23.º do Código da Publicidade, aprovado pelo Decreto-Lei n.º 330/90, de 23 de Outubro.

4 Para efeitos da presente lei, considera-se publicidade:
a) Qualquer forma de comunicação feita por entidades de natureza pública ou privada, no âmbito de uma atividade comercial, industrial, artesanal ou liberal, com o objetivo direto ou indireto de promover, com vista à sua comercialização ou alienação, quaisquer bens ou serviços ou promover ideias, princípios, iniciativas ou instituições;

b) Qualquer forma de comunicação da Administração Pública, não prevista na alínea anterior, que tenha por objetivo, direto ou indireto, promover o fornecimento de bens ou serviços.

5. Para efeitos da presente lei, não se considera publicidade a propaganda política.

Artigo 2.º Identificabilidade exterior
A publicidade entregue no domicílio do destinatário, por via postal ou por distribuição direta, deve ser identificável exteriormente de forma clara e inequívoca, designadamente contendo os elementos indispensáveis para uma fácil identificação do anunciante e do tipo de bem ou serviço publicitado.

Artigo 3.º Publicidade domiciliária não endereçada
É proibida a distribuição direta no domicílio de publicidade não endereçada sempre que a oposição do destinatário seja reconhecível

no ato de entrega, nomeadamente através da afixação, por forma visível, no local destinado à receção de correspondência, de dístico apropriado contendo mensagem clara e inequívoca nesse sentido.

Artigo 4.º Publicidade domiciliária endereçada

1. É proibido o envio de publicidade endereçada para o domicílio, por via postal ou por distribuição direta, quando o destinatário tenha expressamente manifestado o desejo de não receber material publicitário.

2. Para efeitos do disposto no número anterior, as pessoas que não desejarem receber publicidade endereçada têm o direito de se opor, gratuitamente, a que o seu nome e endereço sejam tratados e utilizados para fins de mala direta ou de serem informadas antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de marketing direto ou utilizados por conta de terceiros, em termos idênticos aos previstos na alínea b) do artigo 12.º da Lei n.º 67/98, de 26 de Outubro.

3. As entidades que promovam o envio de publicidade para o domicílio manterão, por si ou por organismos que as representem, uma lista das pessoas que manifestaram o desejo de não receber publicidade endereçada.

4. Com vista à maior eficácia do sistema previsto no número anterior, o Governo apoiará a constituição de listas comuns, nacionais ou sectoriais, da responsabilidade das associações representativas dos sectores interessados ou de operadores de telecomunicações.

5. Os titulares de listas de endereços utilizadas para efeitos de mala direta devem mantê-las atualizadas, eliminando trimestralmente os nomes constantes da lista referida no número anterior.

6. Os prestadores de serviços postais não podem ser considerados coautores para efeitos do disposto no n.º 1 nem se consideram abrangidos pelo dever consagrado no n.º 3, exceto quando eles próprios promovam o envio de publicidade para o domicílio.

Artigo 5.º Publicidade por telefone e telecópia
1. É proibida a publicidade por telefone, com utilização de sistemas automáticos com mensagens vocais pré-gravadas, e a publicidade por telecópia, salvo quando o destinatário a autorize antes do estabelecimento da comunicação, nos termos do artigo 12.º da Lei n.º 69/98, de 28 de Outubro.

2. As pessoas que não desejarem receber publicidade por telefone podem inscrever o número de telefone de assinante de que são titulares numa lista própria, a criar nos termos dos números seguintes.
3. As entidades que promovam a publicidade por telefone manterão, por si ou por organismos que as representem, uma lista das pessoas que manifestem o desejo de não receber essa publicidade, lista essa que deverá ser atualizada trimestralmente.

4. É proibida qualquer publicidade por chamada telefónica para os postos com os números constantes da lista referida nos números anteriores.

5. Os prestadores do serviço de telefone não podem ser considerados coautores para efeitos do disposto nos n.^{os} 1 e 4 nem se consideram abrangidos pelo dever consagrado no n.º 3, exceto quando eles próprios promovam a publicidade por telefone.

Artigo 6.º Proteção dos dados pessoais
Os dados constantes das listas de pessoas referidas nos artigos 4.º e 5.º gozam de proteção, nos termos da Lei n.º 67/98, de 26 de Outubro.

Artigo 7.º Exclusão
O disposto nos artigos anteriores não se aplica:
a) À publicidade entregue no mesmo invólucro conjuntamente com outra correspondência;

b) À publicidade dirigida a profissionais;

c) Quando existam relações duradouras entre anunciante e destinatário, resultantes do fornecimento de bens ou serviços.

Artigo 8.º Sanções
1. Constitui contraordenação, punível com coima de 200 000$ a 500 000$ ou de 400 000$ a 6 000 000$[98], consoante se trate, respetivamente, de pessoas singulares ou de pessoas coletivas, a infração ao disposto nos artigos 2.º, 3.º, 4.º e 5.º, n.os 1, 3 e 4.

2. Podem ainda ser aplicadas as sanções acessórias previstas no artigo 35.º do Código da Publicidade.

3. A negligência é sempre punível, nos termos gerais.

4. É aplicável, com as necessárias adaptações, o disposto no artigo 36.º do Código da Publicidade.

Artigo 9.º Fiscalização de processos e divulgação da lei
1. A fiscalização do cumprimento do disposto no presente diploma e a instrução dos respetivos processos de contraordenação competem ao Instituto do Consumidor.

2. O Instituto do Consumidor, em colaboração com os organismos representativos das entidades que promovam o envio de publicidade para o domicílio ou a publicidade por telefone, realizará ações de divulgação dos direitos conferidos aos cidadãos pela presente lei e demais disposições aplicáveis, incluindo a informação sobre as entidades junto das quais devem ser depositadas as manifestações de vontade de não receber publicidade e o procedimento adequado para exprimir a objeção.

3. O Instituto do Consumidor editará e porá à disposição do público, designadamente através das entidades prestadoras de serviços postais, dísticos que exprimam de forma clara e inequívoca objeção à receção de publicidade.

Artigo 10.º Aplicação de sanções
1. A aplicação das coimas previstas no presente diploma compete à comissão de aplicação de coimas em matéria de publicidade, prevista no artigo 39.º do Código da Publicidade.

---

[98] € 997,60 a € 2.493,99 ou de € 1.995,19 a € 29.927,87.

2. A aplicação das sanções acessórias previstas na presente lei compete ao membro do Governo que tenha a seu cargo a tutela da proteção do consumidor, salvo no caso da sanção acessória prevista na alínea a) do n.º 1 do artigo 35.º do Código da Publicidade, que compete à comissão de aplicação de coimas em matéria de publicidade.

Artigo 11.º Receitas das coimas
As receitas das coimas revertem em 40% para o Instituto do Consumidor e em 60% para o Estado.

Aprovada em 17 de Dezembro de 1998.

O Presidente da Assembleia da República,
António de Almeida Santos.

Promulgada em 11 de Janeiro de 1999.

Publique-se.

O Presidente da República,
JORGE SAMPAIO.

Referendada em 25 de Janeiro de 1999.

22. Decreto-Lei n.º 57/2008, de 26 de Março
estabelece o regime aplicável às práticas comerciais desleais das empresas nas relações com os consumidores, ocorridas antes, durante ou após uma transação comercial relativa a um bem ou serviço, transpondo para a ordem jurídica interna a Diretiva n.º 2005/29/CE, do Parlamento Europeu e do Conselho, de 11 de Maio, relativa às práticas comerciais desleais das empresas nas relações com os consumidores no mercado interno (Alínea c), do artigo 12.º e artigo 21.º)

CAPÍTULO I
PRÁTICAS COMERCIAIS DESLEAIS

(…)

Artigo 12.º Práticas comerciais consideradas agressivas em qualquer circunstância
São consideradas agressivas, em qualquer circunstância, as seguintes práticas comerciais:

(…)

c) Fazer solicitações persistentes e não solicitadas, por telefone, fax, e-mail ou qualquer outro meio de comunicação à distância, exceto em circunstâncias e na medida em que tal se justifique para o cumprimento de obrigação contratual;

(…)

CAPÍTULO II
REGIME SANCIONATÓRIO

Artigo 21.º Contraordenações
1. A violação do disposto nos artigos 4.º a 12.º constitui contraordenação punível com coima de (euro) 250 a (euro) 3740,98, se o infrator for pessoa singular, e de (euro) 3000 a (euro) 44 891,81, se o infrator for pessoa coletiva.

2. São, ainda, aplicáveis, em função da gravidade da infração e da culpa do

agente, as seguintes sanções acessórias:
a) Perda de objetos pertencentes ao agente;

b) Interdição do exercício de profissões ou atividades cujo exercício dependa de título público ou de autorização ou homologação de autoridade pública;

c) Encerramento de estabelecimento cujo funcionamento esteja sujeito a autorização ou licença de autoridade administrativa;

d) Publicidade da aplicação das coimas e das sanções acessórias, a expensas do infrator.

3. As sanções referidas nas alíneas a) a c) do número anterior têm a duração máxima de dois anos contados a partir da decisão condenatória final.

4. A negligência é sempre punível, sendo os limites máximos e mínimos das coimas reduzidos a metade.

5. A fiscalização do cumprimento do disposto no presente decreto-lei, bem como a instrução dos respetivos processos de contraordenação, compete à ASAE ou à autoridade administrativa competente em razão da matéria, conforme o disposto no artigo 19.º

6. A aplicação das coimas compete à entidade prevista no respetivo regime regulador sectorial ou, caso não exista, à Comissão de Aplicação das Coimas em Matéria Económica e de Publicidade (CACMEP).

7. O montante das coimas aplicadas é distribuído nos termos previstos no respetivo regime regulador sectorial ou, caso não exista, da seguinte forma:
a) 60 % para o Estado;

b) 30 % para a entidade que realiza a instrução;

c) 10 % para a entidade prevista no respetivo regime regulador sectorial ou, caso não exista, para a CACMEP.

<u>*23.* Isenções de Notificação</u>
(artigo 27.º, n.º 2, da Lei de Proteção de Dados Pessoais)

I. AUTORIZAÇÃO DE ISENÇÃO N.º 1/99

PROCESSAMENTO DE RETRIBUIÇÕES, PRESTAÇÕES, ABONOS DE FUNCIONÁRIOS OU EMPREGADOS

Artigo 1.º Finalidade do tratamento
Estão isentos de notificação à CNPD os tratamentos automatizados, relativamente a funcionários ou empregados, que tenham como finalidade exclusiva:
a) O cálculo e pagamento de retribuições, prestações acessórias, outros abonos e gratificações;

b) O cálculo, retenção na fonte e operações relativas a descontos na retribuição, obrigatórios ou facultativos, decorrentes de disposição legal;
c) Convenção coletiva de trabalho, pedido formulado pelo trabalhador ou decisão judicial;

d) O cálculo da participação nos lucros da empresa, nos termos da legislação aplicável;

e) A realização de operações estatísticas não nominativas relacionadas com o processamento de salários no âmbito da entidade processadora;

Artigo 2.º Categorias de dados
Os dados tratados deverão ser os estritamente necessários à realização das finalidades referidas no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: o nome, data de nascimento, naturalidade, filiação, sexo, nacionalidade, morada e telefone, habilitações literárias, número de bilhete de identidade, número de contribuinte, número de segurança social, número de sócio do sindicato;

b) Situação familiar: estado civil, nome do cônjuge, filhos ou pessoas a cargo e outras informações suscetíveis de determinar a atribuição de complementos de remuneração;

c) Sobre a atividade profissional: horário e local de trabalho, número de identificação interno, data de admissão, antiguidade, categoria profissional, antiguidade na categoria, nível/escalão salarial, natureza do contrato;

d) Elementos relativos à retribuição: retribuição base, outras prestações certas ou variáveis, subsídios, férias, assiduidade e absentismo, licenças, outros elementos relativos à atribuição de complementos de retribuição, montante ou taxa em relação aos descontos obrigatórios ou facultativos;

e) Outros dados: grau de incapacidade do trabalhador ou de membro do agregado familiar, incapacidade temporária resultante de acidente de trabalho ou de doença profissional, local de pagamento, número de conta bancária, número de associado e identificação da entidade à ordem da qual devem ser efetuados descontos obrigatórios ou facultativos (sindicato, serviços sociais, grupo desportivo, etc.).

Artigo 3.º Prazo de Conservação
1. A informação não poderá ser conservada para além de 10 anos sobre a cessação da relação de trabalho.

2. A informação sobre o motivo da ausência não poderá ser conservada para além do prazo necessário à elaboração do recibo de pagamento da remuneração, nem para além do prazo de prescrição do procedimento disciplinar quando esteja em causa a apreciação de faltas injustificadas.

3. O prazo especificado no n.º 1 não prejudica a conservação dos dados estritamente necessários à prova da qualidade de trabalhador, tempo de serviço e evolução salarial, para efeitos de previdência ou para pagamento de prestações complementares posteriores devidas em momento posterior à cessação da relação de trabalho.

Artigo 4.º Destinatários das informações
1. No âmbito das suas atribuições, apenas podem ser destinatários dos dados:
- As entidades a quem os dados devam ser comunicados por força de disposição legal ou a pedido do titular dos dados;
- As instituições financeiras que gerem as contas da entidade responsável pelo pagamento da retribuição e do trabalhador;
- As Sociedades Gestoras de Fundos de Pensões, desde que o trabalhador

tenha sido informado;
- As Companhias de Seguros quando estiver em causa a celebração de contrato de seguro de acidentes de trabalho ou de acidentes pessoais;
- As entidades que, por força de disposição legal, estão encarregadas de processamento das estatísticas oficiais;

2. Não estarão isentos de notificação os tratamentos automatizados que comuniquem dados a entidades e em circunstâncias diferentes das indicadas no número anterior ou que procedam ao fluxo transfronteiras de dados pessoais.

Artigo 5.º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro

II. AUTORIZAÇÃO DE ISENÇÃO N.º 2/99

GESTÃO DE UTENTES DE BIBLIOTECAS E ARQUIVOS

Artigo 1.º Finalidade do tratamento
Estão isentos de notificação à CNPD os tratamentos automatizados destinados exclusivamente à gestão de utentes de bibliotecas e arquivos.
Artigo 2.º Categorias de Dados
Os dados pessoais tratados devem ser os estritamente necessários à realização da finalidade referida no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: Nome, morada, idade, número de bilhete de identidade, número de leitor ou utente, telefone, fax, e-mail, profissão e habilitações literárias;

b) Outros dados: material requisitado, data de levantamento e data de entrega.

Artigo 3.º Prazo de Conservação
1. O prazo máximo da conservação dos dados é de:
a) Dados de identificação: um ano após o último pedido de requisição por parte do utente ou, caso exista, findo o prazo de caducidade do cartão de leitor;

b) Outros dados: Um ano após a entrega do material requisitado.

2. O prazo previsto no n.º 1 não prejudica a conservação dos dados caso haja pendência de ação judicial por incumprimento das obrigações de utente, com limite de três meses após trânsito em julgado.

Artigo 4.º Destinatários dos Dados
No âmbito das suas atribuições apenas podem ser destinatários dos dados as entidades a quem os dados devam ser comunicados por força de disposição legal.

Artigo 5.º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro.

III. AUTORIZAÇÃO DE ISENÇÃO N.º 3/99

FATURAÇÃO E GESTÃO DE CONTACTOS COM CLIENTES, FORNECEDORES E PRESTADORES DE SERVIÇOS

Artigo 1.º Finalidade do tratamento
Estão isentos de notificação à CNPD os tratamentos automatizados com a finalidade exclusiva de faturação, gestão de contactos com clientes, fornecedores e prestadores de serviços.

Artigo 2.º Categorias de Dados
Os dados pessoais tratados devem ser os estritamente necessários à realização da finalidade referida no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: Nome, data de nascimento, morada, telefone, fax, e-mail, número de identificação fiscal e número de identificação bancária;

b) Outros dados: os referidos no n.º 5 do art.º 38º do Código do IVA, bem como os meios de pagamento, instituição financeira, número de apólice e entidade seguradora, no caso de recurso a entidades seguradoras no âmbito da finalidade prevista no art.º 1º.

Artigo 3º Prazo de Conservação
Os dados pessoais podem ser conservados pelo período máximo de 10 anos, sem prejuízo da sua conservação, para além daquele prazo, em caso de pendência de ação judicial, com limite de três meses após trânsito em julgado.

Artigo 4.º Destinatários dos Dados
São destinatários dos dados as entidades a quem estes devam ser comunicados por força de disposição legal, ou aquelas a quem, contratualmente, o titular dos dados consinta a comunicação, no âmbito da finalidade prevista no art.º 1º.

Artigo 5.º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro.

IV. AUTORIZAÇÃO DE ISENÇÃO N.º 4/99

GESTÃO ADMINISTRATIVA DE FUNCIONÁRIOS, EMPREGADOS E PRESTADORES DE SERVIÇOS

Artigo 1.º Finalidade do tratamento
Estão isentos de notificação à CNPD os tratamentos automatizados que tenham por finalidade exclusiva a gestão administrativa de funcionários, empregados e prestadores de serviços.

Artigo 2.º Categorias de Dados
Os dados pessoais tratados devem ser os estritamente necessários à realização da finalidade referida no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: Nome, idade, número de bilhete de identidade, morada, telefone, fax, e-mail, número de identificação interno e fotografia;

b) Outros dados: Habilitações literárias e profissionais, funções exercidas, categoria, situação profissional e local de trabalho.

Artigo 3º Prazo de Conservação
1. Os dados pessoais podem ser conservados por período máximo de um

ano após a cessação do vínculo laboral à entidade, sem prejuízo da sua conservação em caso de procedimento judicial, para além daquele prazo, até ao limite de seis meses após o trânsito em julgado.

2. Os dados podem ainda ser conservados para fins históricos.

Artigo 4.º Destinatários dos Dados
São destinatários dos dados as entidades a quem estes devam ser comunicados por força de disposição legal.

Artigo 5.º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro.

V. AUTORIZAÇÃO DE ISENÇÃO N.º 5/99

REGISTO DE ENTRADAS E SAÍDAS DE PESSOAS EM EDIFÍCIOS

Artigo 1.º Finalidade do tratamento
1. Estão isentos de notificação à CNPD os tratamentos automatizados que tenham por finalidade exclusiva o registo de entradas e saídas de pessoas em edifícios.

2. A isenção prevista no número anterior não abrange o registo obtido através de câmaras de vídeo.

Artigo 2.º Categorias de Dados
Os dados pessoais tratados devem ser os estritamente necessários à realização da finalidade referida no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: Nome, tipo e número de documento de identificação;

b) Outros dados: hora de entrada e de saída, local, pessoa a contactar, motivo da visita e, nas situações aplicáveis, dados referentes ao veículo.

Artigo 3º Prazo de Conservação
Os dados pessoais não podem ser conservados por período superior a seis meses.

Artigo 4.º Destinatários dos Dados
Os dados pessoais não podem ser comunicados a terceiros, salvo autorização legal que o permita.

Artigo 5º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro.

VI. AUTORIZAÇÃO DE ISENÇÃO N.º 6/99

COBRANÇA DE QUOTIZAÇÕES EM ASSOCIAÇÕES E CONTACTOS COM OS RESPETIVOS ASSOCIADOS

Artigo 1.º Finalidade do tratamento
Estão isentos de notificação à CNPD, desde que autorizados pelo titular, os tratamentos automatizados destinados exclusivamente à cobrança de quotizações e contactos com os associados no âmbito da atividade estatutária da Associação, independentemente da sua natureza, designadamente os efetuados por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical.

Artigo 2.º Categorias de Dados
Os dados tratados deverão ser os estritamente necessários à realização das finalidades referidas no artigo anterior, limitando-se às seguintes categorias de dados:
a) Dados de identificação: Nome, morada, idade, número de bilhete de identidade, número de contribuinte, número de sócio, telefone, fax, e-mail, filiação, profissão, habilitações literárias;

b) Situação familiar: Estado civil, nome do cônjuge, nome dos dependentes e nome e contactos dos encarregados de educação em caso de menores;

c) Outros dados: valor da quota, N.I.B., instituição bancária, situação perante a associação e cargo exercido.

Artigo 3.º Prazo de Conservação
O prazo máximo da conservação dos dados é de três anos finda a qualidade de sócio, exceto quando haja pendência de ação judicial em caso de incumprimento das obrigações de associado.

Artigo 4.º Destinatários dos Dados
No âmbito das suas atribuições apenas podem ser destinatários dos dados:
a) Entidades a quem os dados devam ser comunicados por força de disposição legal ou estatutária;

b) Instituições bancárias para pagamento das respetivas quotas;

c) Companhias de Seguros quando estiver em causa a celebração de contrato de seguro.

Artigo 5.º Direito de Informação
A presente isenção não prejudica a obrigação do responsável do ficheiro quanto ao direito de informação, constante no artigo 10º da Lei 67/98, de 26 de Outubro.

TELL A STORY

ISBN 978-989-99008-4-4