



LEGISLAÇÃO E MECANISMOS DE REGULAMENTAÇÃO DO NEGÓCIO ELECTRÓNICO



FICHA TÉCNICA

Título

*LEGISLAÇÃO E MECANISMOS
DE REGULAMENTAÇÃO
DO NEGÓCIO ELECTRÓNICO*

Autores

Manuel Lopes Rocha, Sónia Queiroz Vaz
e Filipe Viana Lousa

Editor

© SPI – Sociedade Portuguesa de Inovação
Consultadoria Empresarial e Fomento da Inovação, S.A.
Edifício «Les Palaces», Rua Júlio Dinis, 242,
Piso 2 – 208, 4050 PORTO
Tel.: 226 076 400, Fax: 226 099 164
spiporto@spi.pt; www.spi.pt
Porto • 2006

Produção Editorial

Principia
Av. Marques Leal, 21
2775-495 S. João do Estoril
Tel.: +351 214 678 710; Fax: +351 214 678 719
encomendas@principia.pt
www.principia.pt

Projecto Gráfico e Design

Mónica Dias

Impressão

Rolo e Filhos, Artes Gráficas, Lda.

ISBN 972-8589-69-7

Depósito Legal 249617/06

Projecto apoiado pelo Programa Operacional Plurifundos da
Região Autónoma da Madeira (POPRAMIII), co-financiado pelo
Estado Português, e pela União Europeia, através do Fundo
Social Europeu.

NEGÓCIO ELECTRÓNICO

LEGISLAÇÃO E MECANISMOS DE REGULAMENTAÇÃO DO NEGÓCIO ELECTRÓNICO

Manuel Lopes Rocha | Sónia Queiroz Vaz | Filipe Viana Lousa



Sociedade Portuguesa de Inovação

C A P Í T U L O

A Lei do Comércio Electrónico

O B J E C T I V O S

- Delimitar o objecto e âmbito de aplicação da Lei do Comércio Electrónico
- Identificar os prestadores de serviços da sociedade da informação
- Definir os pressupostos de aplicação do regime jurídico da responsabilidade dos prestadores de serviços em rede
- Conhecer os limites legais às actividades de *marketing* directo e publicidade em rede
- Compreender os processos de celebração de contratos por via electrónica e os princípios associados

O desenvolvimento da sociedade da informação potenciou de maneira excepcional as possibilidades de interacção entre os indivíduos e aumentou o número de intervenientes que tomam parte no funcionamento da Internet. Os actores que actuam no espaço virtual, a que chamamos ciberespaço, jamais perdem a sua particular susceptibilidade de serem titulares de direitos e obrigações e sujeitos de relações jurídicas. Como em todas as relações jurídicas, também naquelas que se estabelecem pelos meios cibernéticos existe exercício de direitos e cumprimento (ou incumprimento) de obrigações. O comércio electrónico e os serviços da sociedade da informação constituem uma oportunidade para estimular o crescimento económico e o investimento na inovação por parte das empresas europeias, bem como para reforçar a competitividade da indústria europeia. Consciente destes factores e com o objectivo de eliminar as divergências entre as legislações nacionais que impediam o desenvolvimento dos serviços da sociedade de informação e o funcionamento do mercado interno europeu, a União Europeia optou por regular certos aspectos da sociedade da informação, em especial do comércio electrónico, através da Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000. Este diploma comunitário foi transposto para a ordem jurídica portuguesa pelo Decreto-Lei n.º 7/2004, de 7 de Janeiro, que, em síntese, regula o exercício de actividades económicas na Internet, o regime de responsabilidade dos prestadores intermediários de serviços, as comunicações publicitárias em rede e a contratação electrónica.

OBJECTO E ÂMBITO DE APLICAÇÃO

O Decreto-Lei n.º 7/2004, de 7 de Janeiro, habitualmente designado como Lei do Comércio Electrónico (LCE), transpõe para a ordem jurídica portuguesa a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial, do comércio electrónico, no mercado interno.

Em suma, a LCE visa:

- assegurar a liberdade de exercício de actividades económicas na Internet;
- determinar o regime de responsabilidade dos prestadores intermediários de serviços;
- regular as comunicações publicitárias em rede; e
- regular a contratação electrónica.

Porém, como se esclarece no preâmbulo da LCE, «na tarefa de transposição, optou-se por afastar soluções mais amplas e ambiciosas para a regulação do sector em causa, tendo-se adoptado um diploma cujo âmbito é fundamentalmente o da directiva». Ora, a directiva sobre comércio electrónico, não obstante a sua designação, não regula todo o comércio electrónico. Assim, exclui-se do âmbito de aplicação da LCE a matéria fiscal, a disciplina da concorrência, o regime do tratamento de dados pessoais e da protecção da privacidade, o patrocínio judiciário, os jogos de fortuna, incluindo lotarias e apostas, em que é feita uma aposta em dinheiro, e a actividade notarial ou equiparadas, enquanto caracterizadas pela fé pública ou por outras manifestações de poderes públicos.

PRESTADORES DE SERVIÇOS DA SOCIEDADE DA INFORMAÇÃO

NOÇÃO

Além dos *internautas*, vários intervenientes participam, das mais variadas maneiras, na transmissão e circulação de informação na Internet. Consequentemente, é imperativo averiguar qual a função desempenhada por determinado sujeito na Internet e quais os serviços que oferece aos seus utilizadores. Não se pode ignorar o facto de uma única entidade poder desenvolver várias actividades em simultâneo e proporcionar aos seus utilizadores diferentes tipos de serviços. Contudo, a distinção dos *actores* da Internet segundo as suas funções é particularmente importante, já que a sua eventual responsabilidade dependerá não tanto do seu *status*, mas da actividade por si efectivamente desempenhada. Esta análise funcional é o ponto de partida necessário para a análise que nos propomos efectuar nos pontos seguintes. Assim, para efeitos de responsabilidade distinguiremos entre:

- operador de telecomunicações, que corresponde à entidade que providencia as infra-estruturas que permitem a transmissão de dados em rede, ou seja, a entidade que fornece e mantém os cabos e as linhas telefónicas que interligam todos os servidores da Internet e ligam os computadores dos fornecedores de conteúdos e utilizadores à rede;
- fornecedor de acesso, que corresponde à entidade que proporciona aos utilizadores a ligação à rede, isto é, que permite o seu

acesso à Internet, bem como a outros serviços, como por exemplo, serviços de correio electrónico;

- fornecedor de serviços de armazenagem, que corresponde à entidade que disponibiliza aos utilizadores da rede espaço na memória dos seus servidores para aí colocarem qualquer tipo de conteúdo, como, por exemplo, uma página de Internet, que por sua vez pode incorporar qualquer tipo de material como textos, gráficos, som, programas de computador, etc.;
- fornecedor de instrumentos de busca, que, em sentido amplo, inclui os fornecedores de motores de busca (*search engine*), isto é, programas de computador específicos que permitem aos seus utilizadores pesquisar determinada informação na Internet, com base em palavras ou expressões-chave por si indicadas; e os fornecedores de ligações de hipertexto, conhecidas como hiperligações, que permitem ao utilizador a mudança directa da página da Internet em que estão, ou mesmo de um sítio para outro da rede, sem ter de escrever o endereço electrónico pretendido.
- fornecedor de conteúdos, que corresponde à entidade que coloca a informação disponível em rede e acessível a qualquer utilizador da Internet.

Estes intervenientes integram-se na categoria mais ampla dos prestadores de serviços da Internet (*Internet service provider*), que de uma forma geral definiremos como todas as pessoas singulares ou colectivas que, com fim lucrativo, prestam um serviço no âmbito do funcionamento e utilização da Internet, de uma forma organizada, e com carácter permanente¹.

Excluindo o fornecedor de conteúdo (*content provider*) – que coloca os conteúdos por si seleccionados em rede, à disposição dos utilizadores, e desenvolve uma actividade que transcende já a mera operação de intermediação técnica –, todos os outros prestadores de serviços mencionados podem ser designados como prestadores de serviços intermediários, na medida em que não são autores, nem seleccionam a informação transmitida na Internet, mas apenas *interferem na colocação, no armazenamento e acesso de dados em rede*². É pois a responsabilidade destes últimos que nos irá ocupar na secção seguinte.

De acordo com o artigo 2.º, alínea b), da Directiva sobre o Comércio Electrónico, considera-se prestador de serviços «qualquer pessoa,

singular ou colectiva, que preste um serviço no âmbito da sociedade da informação». Trata-se de uma definição muito ampla que permite incluir não apenas os operadores, mas também os próprios internautas que, ocasionalmente, prestem serviços em rede, sem carácter profissional e até de forma gratuita³.

A LCE veio, no entanto, precisar a noção definindo como «“serviço da sociedade da informação” qualquer serviço prestado a distância por via electrónica, mediante remuneração ou pelo menos no âmbito de uma actividade económica na sequência de pedido individual do destinatário» (artigo 3.º, n.º 1). Por destinatário do serviço deverá aqui entender-se a pessoa que utiliza um serviço da sociedade da informação para transmitir e/ou aceder a determinada informação⁴.

O prestador de serviços considerar-se-á estabelecido em Portugal quando exerça uma actividade económica no país mediante um estabelecimento efectivo, «seja qual for a localização da sua sede» (artigo 4.º, n.º 2). Esclarece ainda a LCE que a mera disponibilização de meios técnicos e de tecnologias necessários para prestar o serviço não constitui, por si só, um estabelecimento efectivo. Saliente-se que «os prestadores de serviços da sociedade da informação estabelecidos em Portugal ficam integralmente sujeitos à lei portuguesa relativa à actividade que exercem, mesmo no que concerne a serviços da sociedade da informação prestados noutro país comunitário» (artigo 4.º, n.º 1).

Por fim, cumpre ainda caracterizar os prestadores intermediários de serviços em rede, definindo-se estes como aqueles 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 4.º, n.º 5). Estes prestadores de serviços têm apenas um papel instrumental na transmissão e difusão de conteúdos de terceiros, não os seleccionando nem tomando parte na decisão de os transmitir em rede. Entre outros, é o caso dos fornecedores de acesso à rede, dos fornecedores de armazenagem e dos fornecedores de serviços de ligações hipertexto e motores de busca.

PRINCÍPIO DA LIBERDADE DE EXERCÍCIO

De acordo com a LCE, é livre o exercício de actividades económicas na Internet, não dependendo de uma autorização prévia a actividade de prestador de serviços da sociedade da informação (artigos 3.º, n.º 3, e 5.º, n.º 2).

O princípio da liberdade de exercício aplica-se a todas as actividades comerciais e profissionais, com excepção das actividades que exi-

gem uma autorização prévia para o seu exercício (por exemplo, a prestação de serviços financeiros, a prestação de serviços de radiodifusão, actividades de jogo) e das profissões que se encontram regulamentadas (por exemplo, advocacia, medicina)⁵. Advirta-se que os prestadores intermediários de serviços em rede que pretendam exercer estavelmente a sua actividade em Portugal devem primeiro proceder à inscrição junto da entidade de supervisão central. Contudo, a mencionada inscrição não se confunde com nenhuma espécie de autorização, pois os prestadores intermediários de serviços não estão sujeitos a nenhum juízo de adequação ou idoneidade por parte das entidades administrativas⁶.

Acrescente-se que os prestadores de serviços se encontram subordinados ao princípio do país de origem, ou seja, encontram-se sujeitos à lei do lugar do estabelecimento. Ora, este princípio aplica-se não só aos prestadores de serviços estabelecidos em Portugal, mas também aos prestadores de serviços estabelecidos noutro Estado-membro da União Europeia, exclusivamente no que respeita a actividades em linha, nomeadamente habilitações, autorizações e notificações, identificação, responsabilidade e exercício, designadamente quanto à qualidade e ao conteúdo dos serviços, à publicidade e aos contratos. Assim, os serviços prestados em Portugal por operadores estabelecidos noutros Estados-membros na União Europeia não estão sujeitos a requisitos adicionais em Portugal, favorecendo-se assim os países mais avançados no comércio electrónico, relativamente aos países receptores⁷.

Porém, o princípio da liberdade de exercício de actividades económicas na Internet consagrado na LCE não tem carácter absoluto, encontrando-se fora do seu âmbito várias matérias (artigo 6.º), designadamente:

- a propriedade intelectual, incluindo a protecção das bases de dados e das topografias dos produtos semicondutores;
- a emissão de moeda electrónica;
- a publicidade realizada por um organismo de investimento colectivo em valores mobiliários;
- a actividade seguradora, quanto a seguros obrigatórios, alcance e condições da autorização da entidade seguradora e empresas em dificuldade ou em situação irregular;
- a matéria disciplinada por legislação escolhida pelas partes no uso da autonomia privada;

- os contratos celebrados com consumidores, no que respeita às obrigações deles emergentes;
- a validade dos contratos em função da observância de requisitos legais de forma, em contratos relativos a direitos reais sobre imóveis;
- a permissibilidade do envio de mensagens publicitárias não solicitadas por correio electrónico.

Desta forma, é, pois, permitido ao Estado-membro em que o serviço é prestado impor a essa mesma prestação os requisitos constantes da sua legislação nacional, restringindo assim a liberdade de prestação de serviços da sociedade da informação⁸. Mas o país de destino do serviço pode ainda recorrer a providências restritivas. Com efeito, os tribunais e outras entidades competentes, nomeadamente, as entidades de supervisão, podem restringir a circulação de um determinado serviço da sociedade da informação proveniente de outro Estado-membro da União Europeia se lesar ou ameaçar gravemente:

- a dignidade humana ou a ordem pública, incluindo a protecção 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;
- a saúde pública;
- a segurança pública, nomeadamente na vertente da segurança e defesa nacionais; e
- os consumidores, incluindo os investidores.

Por fim, refira-se que as providências que venham a ser tomadas nos termos *supra* expostos devem ser proporcionais aos objectivos a tutelar.

RESPONSABILIDADE DOS PRESTADORES DE SERVIÇOS EM REDE

ÂMBITO DE APLICAÇÃO

A LCE, no seu capítulo III (artigos 11.º a 19.º), estabelece o regime da responsabilidade dos prestadores de serviços da sociedade de

informação referente às actividades de simples transporte, armazenagem intermediária, armazenagem principal e de associação de conteúdos (ligações de hipertexto e motores de busca). Prevê-se também que os prestadores de serviços não estejam sujeitos a um dever geral de vigilância das informações que transmitem ou armazenam.

Embora a LCE se refira na epígrafe do seu capítulo III, em geral, à responsabilidade dos prestadores de serviços em rede, o regime aí estabelecido apenas respeita aos prestadores intermediários de serviços em rede, conforme acima os identificámos.

A LCE estabelece o princípio da irresponsabilidade dos prestadores de serviços pela informação que transportem, armazenem ou a que facultem o acesso, enquanto exerçam uma actividade puramente técnica, automática e de natureza passiva. Reconhece-se que nestes casos não é exigível, nem tecnicamente possível, ter conhecimento da informação transmitida ou armazenada, nem o seu controlo. Porém, no caso de serviços armazenagem principal de informações e de associação de conteúdos, a partir do momento em que tenha conhecimento da ilicitude do conteúdo, exige-se que o prestador de serviços proceda com diligência no sentido de remover as informações em causa ou impossibilitar o acesso a elas, sob pena de responder por perdas e danos.

Refira-se ainda que as regras estabelecidas no capítulo III da LCE respeitam tanto a responsabilidade civil, como a penal. No entanto, tenha-se presente que a LCE não estabelece propriamente uma regulação geral de responsabilidade dos prestadores de serviços. Na verdade, estabelece a favor desses intermediários isenções concretas de responsabilidade que actuam como um filtro: só se um prestador de serviços não preencher as condições estipuladas que o exoneram de qualquer responsabilidade é que poderá incorrer em responsabilidade civil ou criminal nos termos das leis gerais⁹.

Por fim, assinala-se que o regime de responsabilidade previsto na LCE, no seguimento da Directiva sobre o Comércio Electrónico, adopta uma abordagem horizontal, ou seja, aplica-se tanto a situações de violação de direito de autor, como a situações de concorrência desleal, publicidade ilícita, difamação, etc.

PRINCÍPIO DA EQUIPARAÇÃO

Antes de mais, importa sublinhar que sem prejuízo das especificações constantes da LCE, a responsabilidade dos prestadores de serviços em rede encontra-se sujeita ao regime comum da responsabilidade,

aplicando-se, consequentemente, as regras gerais. Por outras palavras, o regime de responsabilidade dos prestadores de serviços em rede estabelecido na LCE, que consagra a irresponsabilidade dos prestadores intermediários de serviços, só terá aplicação quando os requisitos nele previstos sejam preenchidos. Caso contrário, aplicar-se-á pois o regime comum da responsabilidade (civil e penal).

Assim, por exemplo, o *fornecedor de conteúdo* que toma a iniciativa de colocar em rede determinada informação ilícita será responsável, perante o titular dos direitos dessa forma violados, pelos danos que, eventualmente, tenha causado com a sua conduta ilícita, nos termos previstos na lei geral (artigos 483.º e seguintes do Código Civil). Este ponto é indiscutível.

Sucedem que logo nos deparamos com um problema de ordem prática: Como conseguir imputar essa conduta danosa e responsabilizar um determinado autor num ambiente virtual em que se movimentam milhões de cibernautas? Constituindo a Internet uma rede informática aberta, a que qualquer indivíduo se pode ligar desde que possua o material adequado e beneficie dos serviços de um fornecedor de acesso, dificilmente se identificará quem colocou ilicitamente a obra em rede.

Mas a responsabilização do autor directo da lesão não será difícil de se concretizar apenas por ele ser desconhecido. Acresce que, atento o carácter internacional da Internet, essa pessoa, mesmo quando identificável, poderá estar, não obstante, domiciliada no estrangeiro, por vezes em países com um ordenamento jurídico bastante diferente, da mesma forma que pode ser insuficiente a garantia geral constituída pelo seu património para efeitos indemnizatórios.

Atentos estes factos, dirigiu-se a atenção para os referidos prestadores de serviços intermediários no funcionamento da *rede*, que providenciam as infra-estruturas da sociedade da informação. Do ponto de vista de quem sofreu o dano, será tentador e mais recompensador agir contra o intermediário da cadeia de comunicação, pois, além de ser muito mais fácil localizar um prestador intermediário de serviços em rede (como acima salientámos, aqueles que estiverem estabelecidos em Portugal estão sujeitos a inscrição junto da entidade de supervisão central), estes prestadores oferecem uma melhor garantia aos titulares dos direitos lesados de serem completamente ressarcidos dos prejuízos sofridos. É neste sentido que a LCE vem regular os termos em que os prestadores intermediários de serviços, que, habitualmente, não intervêm nos conteúdos transmitidos, podem ser responsabilizados, conforme examinaremos de seguida.

RESPONSABILIDADE POR SERVIÇOS DE SIMPLES TRANSPORTE

Entre os vários tipos de actividades exercidas pelos prestadores de serviços da Internet existem dois tipos de prestações que constituem exemplos paradigmáticos de actividades meramente instrumentais: a transmissão, através de uma rede de telecomunicações, de informações prestadas e solicitadas por um terceiro e o simples serviço de proporcionar acesso a uma rede de telecomunicações.

De acordo com a LCE (artigo 14.º, n.º 1), o prestador intermediário que preste estes serviços não será responsabilizado pelas informações transmitidas desde que cumulativamente:

- não esteja na origem da transmissão;
- não selecione o destinatário da transmissão; e
- não selecione nem modifique as informações que são objecto da transmissão.

O primeiro requisito poderá, à primeira vista, criar alguma confusão, já que para que qualquer conteúdo seja transmitido na Internet é sempre necessária, à partida, a intervenção de um prestador de serviços. O que efectivamente se pretende especificar é que prestador de serviços não deve ser o criador do conteúdo da transmissão – caso em que passará a ser um fornecedor de conteúdos e não beneficiará deste regime –, nem o actor que toma a iniciativa de efectuar determinada transmissão¹⁰. A decisão de efectuar uma transmissão parte do destinatário do serviço, que é quem disponibiliza os dados e solicita a sua transmissão.

Quanto ao segundo requisito, note-se que não constitui selecção do destinatário da transmissão o facto de um prestador de serviços enviar um *e-mail* a pedido de um utilizador do serviço para cada um dos utilizadores que integrem uma *mailing list* disponibilizada em linha.

Relativamente ao terceiro requisito, compreende-se a sua exigência. Quando seleccionar ou modificar os conteúdos, o prestador de serviços estará a actuar como um fornecedor de conteúdos e já não como um intermediário. Nesse caso, já não poderá ignorar conhecer os materiais potencialmente ilícitos que transmite. Saliente-se que não constituirá modificação dos conteúdos a manipulação estritamente técnica da informação que ocorre durante o processo de transmissão, nomeadamente a divisão da informação em vários *pacotes* de dados, que se reunificarão ao chegar ao seu destino.

Esclarece ainda a LCE (artigo 14.º, n.º 2) que as actividades de transmissão e fornecimento de acesso isentas de responsabilidade compreendem também a armazenagem automática, intermediária e transitória das informações transmitidas, desde que essa armazenagem vise exclusivamente a execução da transmissão em rede e a sua duração não exceda o tempo considerado razoavelmente necessário.

Concluindo, a isenção para as actividades de simples transporte supõe que o prestador de serviços não esteja implicado de nenhuma maneira na informação transmitida. Esta solução emerge da intenção de se prevenir toda a forma de controlo e censura por parte destes agentes: os operadores da rede ou os fornecedores de acesso devem ser neutros quanto aos conteúdos difundidos e não devem interferir de forma nenhuma neles. A sua responsabilidade civil ou penal não surgirá mesmo quando tenham conhecimento da presença de informação ilícita em rede e, podendo actuar, se abstenham de intervir, o que não implica que o prestador de serviços não seja obrigado a prevenir ou a fazer cessar determinada infracção, quando tal lhe seja exigido por um tribunal ou autoridade administrativa.

RESPONSABILIDADE POR SERVIÇOS DE ARMAZENAGEM INTERMEDIÁRIA

O *caching* ou armazenagem intermediária é, hoje em dia, uma actividade vantajosa para todos os que utilizam a Internet. Ao providenciar-se a armazenagem intermédia e temporária em servidores locais de materiais solicitados com mais frequência, habitualmente disponíveis em servidores remotos, permite-se que o acesso a essa informação seja feito de forma mais rápida, eficaz e a um menor custo. Na verdade, quando outros utilizadores voltarem a reclamar o mesmo conteúdo já não será necessário ir «buscá-lo» ao servidor em que originalmente está armazenado; bastará aceder à cópia que o prestador possui na sua memória *cache*. O *caching*, para todos os efeitos, é uma reprodução, embora temporária, mais longa do que as ocorridas num acto de transmissão. De outra forma ocorreriam congestionamentos de tráfego na rede, tornando mais difícil e moroso o acesso à informação.

Assim, de acordo com a LCE (artigo 15.º), um prestador intermediário de serviços não deverá ser responsabilizado pela armazenagem automática, intermédia e temporária de informação¹¹ prestada por um destinatário do serviço, efectuada apenas com o objectivo de tornar mais eficaz e económica a posterior transmissão dessa informação a pedido de outros utilizadores, desde que: não modifique a informação; respeite as condições de acesso à informação¹²; respeite as regras

relativas à actualização da informação adoptadas pelo sector; não interfira com a utilização legítima da tecnologia com o objectivo de obter dados sobre a utilização da informação¹³; e actue com diligência para remover ou impossibilitar o acesso à informação que armazenou, logo que tome conhecimento efectivo de que esta 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 impossibilidade de acesso.

RESPONSABILIDADE POR SERVIÇOS DE ARMAZENAGEM PRINCIPAL

Os prestadores de serviços intermediários que se limitam a colocar à disposição de utilizadores espaço nos seus servidores, por forma a lhes permitir a colocação de conteúdos – *hosting* – beneficiam também de um limite à sua responsabilidade por actos relacionados com essa armazenagem (artigo 16.º da LCE).

Neste caso, o prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento da ocorrência actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação. Note-se que os prestadores intermediários de serviços não beneficiarão deste regime se o destinatário do serviço que armazenou a informação ilícita tiver agido sob a autoridade ou o controlo daquele, uma vez que pode intervir nesse conteúdo.

Acresce que haverá responsabilidade civil sempre que, perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação. Esta *consciência* do prestador intermediário de serviços aferir-se-á perante aquilo que conhece, ou seja, o prestador de serviços terá de avaliar se uma actividade ou uma informação são ilícitas: se concluir, ou dever concluir, pela ilicitude, tem o dever de retirar ou impedir o acesso à informação, sob pena de incorrer em responsabilidade civil¹⁴.

Concretamente, a LCE estabelece dois requisitos para que o prestador intermediário de serviços de armazenagem principal possa ser responsabilizado, nos termos gerais:

- Em primeiro lugar, a ilicitude da informação armazenada ou actividade deve ser manifesta;
- Em segundo, lugar, o prestador tem de ter conhecimento da actividade ou informação que consubstancia o acto ilícito manifesto.

Todavia, em matéria de propriedade intelectual, dificilmente se encontrarão situações em que a ilicitude é manifesta para um simples operador técnico, como é um prestador intermediário de serviços. Mesmo ponderando a hipótese de um prestador de serviços proceder a acções de supervisão espontâneas, como será ele capaz de avaliar se determinada obra literária ou artística se encontra disponibilizada ao público sem autorização do titular dos direitos de autor? Será suficiente que não se faça menção a essa autorização no sítio em causa? Bastará o facto de determinado sítio disponibilizar obras literárias ou artísticas gratuitamente aos seus utilizadores para que estejamos perante uma actividade suspeita que mereça imediatamente ser interdita, sob pena de responsabilidade do prestador de serviços? As obras em causa podem muito bem encontrar-se no domínio público. Nestes casos, tudo será muito relativo e incerto para que se possa inferir se o prestador de serviços conhecia factos ou circunstâncias que indicavam o carácter ilícito da actividade.

O conhecimento da actividade ou informação que consubstancia um acto ilícito manifesto pode ser obtido quer directamente, quer através da arguição da violação por parte de um interessado. Sucede que a LCE não esclarece o que constitui uma comunicação adequada por parte de um terceiro para que se possa considerar que o prestador de serviços dispõe do conhecimento exigido em ordem a actuar. Será adequada uma comunicação feita por qualquer pessoa, ou, por exemplo, apenas se deverá atender à comunicação do titular dos direitos lesados? Bastará um *e-mail* enviado por um terceiro para que se considere que o prestador tem conhecimento da ilicitude do conteúdo? Do ponto de vista do prestador de serviços, no silêncio da lei, será preferível que, quando receba uma comunicação, actue com prontidão, no sentido de impedir o acesso ou remover a informação presumivelmente ilícita, salvo se a notificação for anónima¹⁵. Em matéria de direito de autor, em que a apreciação da ilicitude do acto, como da titularidade dos direitos, não é fácil, parece ter de se tomar em consideração as comunicações feitas pelas entidades de gestão colectiva, como, por exemplo, a Sociedade Portuguesa de Autores ou a Cooperativa de Gestão dos Direitos dos Artistas Intérpretes ou Executantes (GDA), que, naturalmente, merecerão todo o crédito.

Acrescente-se que a LCE não exonera de responsabilidade os prestadores de serviços que intervenham, prontamente, no sentido de remover a informação alegadamente ilícita e que afinal se vem, posteriormente, a revelar lícita. O prestador de serviços pode ver-se entre dois «fogos»: por um lado, poderá ter de responder perante ter-

ceiros por não ter removido as informações lesivas dos seus direitos; por outro, poderá ter de responder perante os seus clientes por ter removido conteúdos que eram perfeitamente lícitos¹⁶. Assim, deverá agir rapidamente sob pena de incorrer em responsabilidade civil delictual perante os terceiros lesados, sob pena de originar a sua responsabilidade civil contratual face aos seus clientes.

Quando o operador for notificado, por uma autoridade competente, da ilicitude do material armazenado, parece indiscutível que se considerará ter o grau de conhecimento necessário para agir.

Saliente-se ainda que a LCE também não esclarece qual o padrão de diligência exigível ao prestador de serviços para que se exonere de responsabilidade: remover o material ilícito em oito dias, em 15 dias? Cremos que o padrão de diligência exigível dificilmente poderá ser fixado por lei. A sua determinação deverá ser efectuada individualmente, caso a caso, pela jurisprudência, não deixando de se atender às concretas capacidades técnicas de cada operador e à consequente possibilidade de actuar.

RESPONSABILIDADE POR SERVIÇOS DE ASSOCIAÇÃO DE CONTEÚDOS

Segundo a LCE, os prestadores intermediários de serviços de associação de conteúdos em rede, por meio de instrumentos de busca, hiperligações ou processos análogos que permitam o acesso a conteúdos ilícitos, estão sujeitos ao mesmo regime de responsabilidade estabelecido para os serviços de armazenagem principal. Também neste caso se coloca o problema de saber quando é que o prestador de serviços tem o nível de conhecimento legalmente exigido para que incorra na obrigação de suprimir as ligações aos sítios com conteúdos ilícitos ou lesivos, sob pena de responder por perdas e danos.

Ao contrário do que se estabelece a propósito dos prestadores de serviço de armazenagem, aqui nada se refere quanto à aplicabilidade deste regime no caso de o titular do sítio para o qual é dirigida a ligação de hipertexto actuar sob a direcção, autoridade ou o controlo do prestador que facilite a localização de informação. Não cremos que essa menção fosse sequer necessária. Caso exista a relação, não se pode considerar que o prestador de serviços esteja a actuar como intermediário. A sua posição deverá ser caracterizada como fornecedor de conteúdos e a isenção não se aplicará: o prestador de serviços tem efectivo conhecimento dos conteúdos ilícitos para que remete os seus clientes e mesmo assim mantém a ligação ao sítio. Há neste caso

uma nítida identificação entre o prestador de serviços e o sítio para o qual se estabelece a ligação, o que nos permite inferir que o primeiro adopta os conteúdos do segundo.

O que aqui está em causa não é a regularidade ou irregularidade da hiperligação, mas sim a circunstância de as hiperligações permitirem o acesso a conteúdos ilícitos. Por conseguinte, o prestador pode ser responsabilizado, em termos gerais, se a ilicitude for manifesta e se tiver conhecimento da actividade ou o conteúdo que consubstancia o acto ilícito manifesto. Já não pode ser responsabilizado se impossibilitar o acesso ao conteúdo ilícito.

AUSÊNCIA DE UM DEVER GERAL DE VIGILÂNCIA DOS PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS

Chegados a este ponto podemos, com segurança, constatar que o conhecimento da ilicitude da informação constitui o ponto de partida para desencadear o progressivo afastamento do regime de isenção de responsabilidade previsto na LCE, caso o prestador de serviços se abstenha de actuar no sentido de proceder à sua remoção ou bloquear o seu acesso.

Vimos igualmente que em nenhuma passagem se esclarece como poderá surgir esse conhecimento. Observámos, porém, que dificilmente o prestador obterá conhecimento da ilicitude por si. Um dos motivos para que assim suceda reside na já aludida dificuldade técnica destes operadores em controlar a quantidade astronómica de informação que circula pelos seus sistemas. Efectuar este controlo não só é praticamente impossível, como, a ser imposto, conduziria a custos elevadíssimos, dificilmente suportáveis pelos operadores da Internet.

Ora, segundo a LCE, 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. Assim, em geral, os prestadores intermediários de serviços não têm a obrigação de averiguar se os conteúdos que armazenam ou transmitem consubstanciam uma prática ilícita.

DEVERES COMUNS DOS PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS

A circunstância de o prestador intermediário de serviços não estar vinculado a um dever geral de vigilância ou de investigação não implica que não esteja obrigado a, na relação com as entidades de supervisão,

adoptar determinados comportamentos. Recorde-se que, nos termos da LCE, os prestadores intermediários de serviços em rede que pretendam exercer estavelmente a actividade em Portugal devem primeiro proceder à inscrição junto da entidade de supervisão central.

Assim, segundo a LCE, constituem obrigações dos prestadores intermediários de serviços para com as entidades competentes:

- informar de imediato quando tiverem conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam;
- satisfazer os pedidos de identificação dos destinatários dos serviços com quem tenham acordos de armazenagem;
- cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação;
- fornecer listas de titulares de sítios que alberguem, quando lhes for pedido.

SOLUÇÃO PROVISÓRIA DE LITÍGIOS

Atento o *supra* exposto, assim que recebam alguma comunicação de um terceiro informando que determinado conteúdo é ilícito, e, recheando ser considerados responsáveis, se sintam incentivados por normas que lhes garantem imunidade, os prestadores intermediários de serviços tenderão a automática e sistematicamente remover ou bloquear o acesso à informação alegadamente ilícita. Procurando evitar situações incertas, os intermediários actuarão com cautela, o que significa que, à menor suspeita, bloquearão o acesso a determinados sítios que acreditem ser ilícitos, na maioria das vezes sem dar nenhuma possibilidade de protesto ao titular da informação em causa.

Estes comportamentos *diligentes*, no fundo encorajados pela lei, colocam seriamente em risco princípios como a liberdade de expressão, especialmente porque a actuação dos intermediários não é antecedida por uma prévia intervenção de uma autoridade judicial. Recorde-se que a liberdade de expressão constitui não só um direito fundamental garantido constitucionalmente, nos termos do artigo 37.º da Constituição da República Portuguesa, mas também um direito garantido pela Convenção Europeia dos Direitos do Homem.

Nos termos da LCE, a solução para evitar esse tipo de situações passa pela consagração legal de um mecanismo de resolução provisória de litígios. Além disso, sabendo-se que os tribunais judiciais difícil-

mente têm capacidade para a resolução destes litígios de uma forma eficaz, especialmente no que diz respeito à adopção de medidas num curto espaço de tempo, pretendeu-se, ao optar-se por este mecanismo, dotar uma entidade administrativa de competência para decidir provisoriamente se determinados conteúdos devem ser removidos ou se deve ser bloqueado o acesso a informações específicas. Visa-se pois obter a rápida resolução de questões em que a morosidade na adopção de medidas possa ter consequências nefastas e de difícil reparação, nomeadamente para aqueles que são prejudicados pela manutenção do conteúdo ilícito em rede¹⁷.

Sucede que apenas se pode recorrer a esse mecanismo de solução provisória de litígios numa situação de armazenagem principal ou de associação de conteúdos (artigo 18.º, n.º 1, da LCE).

De acordo com a LCE, os prestadores intermediários de serviços de armazenagem principal ou de associação de conteúdos não são obrigados, quando a ilicitude dos conteúdos não for manifesta, a remover o conteúdo contestado ou a impossibilitar o acesso à informação, só pelo facto de um terceiro arguir uma violação (artigo 18.º, n.º 1). Nesses casos, o interessado pode recorrer à entidade de supervisão, que apresentará uma solução provisória em 48 horas, que será imediatamente comunicada aos intervenientes, por via electrónica. Prevê-se também que quem tiver interesse jurídico na manutenção daquele conteúdo em linha possa, nos mesmos termos, recorrer à entidade de supervisão para obter a solução provisória do litígio emergente. Qualquer que seja a decisão, nenhuma responsabilidade recairá sobre a entidade de supervisão e, tão-pouco, sobre o prestador intermediário de serviços por ter ou não retirado o conteúdo ou impossibilitado o seu acesso, desde que não seja manifesta a sua ilicitude. Admite-se que a entidade de supervisão possa, a qualquer momento, alterar a composição provisória do litígio estabelecida. A solução definitiva do litígio será realizada nos termos e pelas vias comuns, ou seja, pelos tribunais.

Porém, ao não se esclarecer o significado de actividade manifestamente ilícita, limita-se imediatamente o campo de aplicação do regime descrito. Senão, vejamos: por um lado, prevê-se uma isenção de responsabilidade quando o prestador de serviços actue diligentemente no sentido de remover ou bloquear o acesso a informação manifestamente ilícita; por outro, isenta-se igualmente o prestador de serviços quando, tratando-se de informação que não é manifestamente ilícita, tenha ou não retirado o conteúdo ou impossibilitado o seu acesso. Se, porventura, o conteúdo em causa vier a ser considerado manifestamente ilícito e o prestador de serviços não tiver retirado ou bloqueado

o acesso ao material em causa, será, eventualmente, responsabilizado. No entanto, se se tratar de um conteúdo de ilicitude duvidosa, tendo o prestador intermediário de serviços retirado ou bloqueado o seu acesso beneficiará de uma isenção de responsabilidade, quer o conteúdo venha a revelar-se manifestamente ilícito ou, pelo contrário, perfeitamente lícito. Sem prejuízo de melhor opinião, os resultados parecem-nos óbvios: na dúvida, o prestador de serviços retirará sempre ou bloqueará o seu acesso ao material. Ao titular do sítio afectado cumprirá recorrer para a entidade de supervisão com vista à solução provisória do litígio. Contudo, não se prevê a obrigatoriedade de o prestador de serviços informar o titular do sítio da sua decisão e dos motivos que estão na sua base. Fica por esclarecer como poderá o terceiro recorrer para a entidade de supervisão de uma decisão cuja fundamentação ignora certamente.

Cumpra ainda salientar a incerteza e insegurança dos intervenientes perante a possibilidade atribuída à entidade de supervisão, de, sem mais e a qualquer momento, poder alterar a composição provisória do litígio.

Refira-se contudo que a LCE prevê que o procedimento perante a entidade de supervisão seja especialmente regulado, o que até à data ainda não sucedeu, inviabilizando-se, assim, a aplicação deste mecanismo de solução provisória de litígios.

COMUNICAÇÕES PUBLICITÁRIAS EM REDE E *MARKETING* DIRECTO

ÂMBITO

É um facto assente que na actividade comercial não basta desenvolver um bom produto, há que o dar a conhecer e valorizar. Este objectivo é concretizado através de uma política de comunicação das empresas dirigida aos seus clientes, aos distribuidores e todos os alvos. A política de comunicação é prosseguida através de vários meios.

Os meios de comunicação de que uma organização pode dispor são numerosos e variados. Entre estes meios de comunicação podemos distinguir a publicidade e o *marketing* directo.

Nos termos do n.º 1 do artigo 3.º do Código da Publicidade, define-se publicidade como «qualquer forma de comunicação feita por enti-

dades de natureza pública ou privada, no âmbito de uma actividade comercial, industrial, artesanal ou liberal, com o objectivo directo ou indirecto de: a) promover, com vista à sua comercialização ou alienação, quaisquer bens ou serviços; b) e promover ideias, princípios, iniciativas ou instituições».

Segundo a Direct Marketing Association, por *marketing* directo entende-se o conjunto das actividades através das quais os bens e serviços são oferecidos a segmentos do mercado por intermédio de um ou vários media, tendo em vista informar ou solicitar uma resposta directa por parte de um potencial ou real cliente, mediante a utilização do correio, do telefone ou de outros meios¹⁸. Saliente-se que em Portugal, o *marketing* directo tende a ser substituído pelo conceito de *marketing* relacional, na medida em que, muitas vezes, o primeiro era conotado de forma negativa e simplista pelos consumidores, que o identificavam com a publicidade não endereçada que invade as nossas caixas de correio¹⁹. De acordo com a APAP – Associação Portuguesa das Agências de Publicidade –, o *marketing* relacional corresponde a toda a forma de publicidade que visa estabelecer e manter relações entre a marca e o seu consumidor com base em acções personalizadas, interactivas e mensuráveis, criando uma base de conhecimento em constante evolução para a construção da marca²⁰.

Ora, de acordo com a LCE, não constituem comunicação publicitária:

- mensagens que se limitem a identificar ou permitir o acesso a um operador económico ou identifiquem objectivamente bens, serviços ou a imagem de um operador, em colectâneas ou listas, particularmente quando não tiverem implicações financeiras, embora se integrem em serviços da sociedade da informação;
- mensagens destinadas a promover ideias, princípios, iniciativas ou instituições.

Considerando o que acima referimos, verificamos que a promoção de ideias, princípios, iniciativas ou instituições constitui, assim, publicidade, para efeitos do Código da Publicidade, não sendo contudo considerada uma comunicação publicitária em rede.

Dispõe ainda a LCE que a comunicação publicitária pode ter somente por fim promover a imagem de um operador comercial, industrial, artesanal ou integrante de uma profissão regulamentada. A caracterização de uma comunicação como publicitária, para este efeito, depende exactamente da intenção de promover o profissional, salientando algum aspecto positivo ou dando a entender a existência de alguma característica especial²¹.

IDENTIFICAÇÃO E INFORMAÇÃO

Em conformidade com a LCE, as comunicações publicitárias prestadas a distância, por via electrónica, devem estar claramente identificadas de modo a serem apreendidas com facilidade por um destinatário comum (artigo 21.º):

- a natureza publicitária, logo que a mensagem seja apresentada no terminal e de forma ostensiva;
- o anunciante;
- as ofertas promocionais, como descontos, prémios ou brindes, e os concursos ou jogos promocionais, bem como os condicionais a que estão submetidos.

Saliente-se que a não-identificação clara dos elementos *supra* identificados, de modo a serem apreendidos com facilidade por um destinatário comum, constitui uma contra-ordenação punível com coima de 2500 a 5000 euros, agravada em um terço nos limites máximo e mínimo se o ilícito for praticado por uma pessoa colectiva [artigo 37.º, n.ºs 1, alínea a), e 5.º da LCE].

COMUNICAÇÕES NÃO SOLICITADAS

A noção de *spam* encontra-se generalizada e corresponde ao envio de comunicações comerciais por via electrónica, para fins publicitários ou de *marketing*, não solicitadas pelo destinatário²².

Sobre esta matéria, estabelece-se na LCE (artigo 22.º) que o envio de mensagens para fins de *marketing* directo, cuja recepção seja independente de intervenção do destinatário, nomeadamente por via de aparelhos de chamada automática, aparelhos de telecópia ou correio electrónico, carece de consentimento prévio do destinatário e a identidade da pessoa responsável pelo envio deve poder ser claramente identificada.

Observamos que o legislador nacional optou por consagrar o regime de opção positiva, que garante que só recebe mensagens não solicitadas quem estiver efectivamente interessado em recebê-las.

Deste regime exceptuam-se, porém, as mensagens enviadas a pessoas colectivas, ficando, no entanto, aberto aos destinatários o recurso ao sistema de opção negativa. Neste sistema, é permitida a difusão de mensagens não solicitadas, excepto se o destinatário se opuser a recebê-las. É também permitido ao fornecedor de um produto ou serviço, no que respeita a estes ou a produtos ou serviços análogos,

enviar publicidade não solicitada aos clientes com quem celebrou anteriormente transacções, se ao cliente tiver sido explicitamente oferecida a possibilidade de o recusar por ocasião da transacção realizada e se não implicar para o destinatário um dispêndio adicional ao custo do serviço de telecomunicações. Em qualquer caso, o destinatário deve ter acesso a meios que lhe permitam a qualquer momento recusar, sem ónus e independentemente de justa causa, o envio dessa publicidade para o futuro. Para esse efeito, cada comunicação electrónica não solicitada deve indicar um endereço e um meio técnico electrónico de fácil identificação e utilização.

Por fim, resta assinalar que cabe às entidades que promovam o envio de comunicações publicitárias não solicitadas e cuja recepção seja independente da intervenção do destinatário manter, por si ou por organismos que as representem, uma lista actualizada de pessoas que manifestaram o desejo de não receber esse tipo de comunicações, não lhes podendo ser enviadas comunicações publicitárias.

PROFISSÕES REGULAMENTADAS

Decorre da LCE (artigo 23.º) que as comunicações publicitárias a distância por via electrónica em profissões regulamentadas (por exemplo, a advocacia) são permitidas mediante o estrito cumprimento das regras deontológicas de cada profissão, nomeadamente as relativas à independência, à honra e ao sigilo profissional, bem como à lealdade para com o público e à lealdade dos membros da profissão entre si. Consequentemente, a publicidade é proibida se assim resultar das regras deontológicas.

CONTRATAÇÃO ELECTRÓNICA

ÂMBITO

O comércio electrónico permite concretizar negócios por via electrónica, abrangendo várias actividades que, entre outras, incluem a compra e venda de bens e serviços e a entrega em linha de conteúdo digital. Em termos negociais, o comércio electrónico consiste na aplicação de meios tecnológicos para a automação de transacções e envio e recepção de dados.

Desde já, assinale-se que, para se conhecer o regime aplicável à contratação electrónica, não é suficiente observar apenas o disposto na LCE. Para além das normas gerais previstas no nosso Código Civil referentes aos contratos, importa também ter em consideração os diplomas legais relativos à protecção dos consumidores.

Porém, as disposições constantes da LCE aplicam-se a todo o tipo de contratos celebrados por via electrónica ou informática, sejam ou não qualificáveis como comerciais.

PRINCÍPIO DA LIBERDADE DE CELEBRAÇÃO

O princípio da liberdade de celebração de contratos por meios electrónicos significa o reconhecimento da declaração electrónica como meio idóneo de manifestação da vontade. Significa ainda que os contratos electrónicos satisfazem a exigência legal de forma escrita, salvo em certos casos, como os negócios familiares (por exemplo, casamento), sucessórios (por exemplo, testamento), reais imobiliários (por exemplo, compra e venda ou hipoteca de imóvel), com excepção do arrendamento, e de caução e garantia, quando não se integrarem na actividade profissional de quem as presta. Excluem-se ainda os negócios jurídicos em que se exija a intervenção de um tribunal, um ente público, um ente que exerça poderes públicos ou um notário. Nesses casos, o negócio jurídico só é válido com a intervenção das referidas entidades.

Resulta ainda do princípio da liberdade de celebração que «só tem de aceitar a via electrónica para a celebração de um contrato quem se tiver vinculado a proceder dessa forma» (artigo 25.º, n.º 3, da LCE). Além disso, são proibidas cláusulas contratuais gerais que imponham a celebração por via electrónica dos contratos com consumidores.

Em matéria de forma, a LCE (artigo 26.º) estabelece expressamente que «as declarações emitidas por via electrónica satisfazem a exigência legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação» e que «o documento electrónico vale como documento assinado quando satisfazer os requisitos da legislação sobre assinatura electrónica e certificação». Sem nos querermos antecipar, uma vez que este tema será tratado mais à frente, diremos apenas que segundo o diploma legal que regula a assinatura digital (Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações em vigor), «o documento electrónico cujo conteúdo seja susceptível de representação como declaração escrita» tem a força probatória de documento particular assinado «quando lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada».

INFORMAÇÕES PRÉVIAS

Qualquer prestador de serviços da sociedade da informação deve disponibilizar permanentemente em linha, mesmo que a sua comunicação não tenha por objecto a contratação, em condições que permitam um acesso fácil e directo, elementos completos de identificação que incluam, nomeadamente:

- nome ou denominação social;
- endereço geográfico em que se encontra estabelecido e endereço electrónico que permitam uma comunicação directa;
- inscrições do prestador em registos públicos e respectivos números de registo;
- número de identificação fiscal.

Acrescente-se que, se exercer uma actividade sujeita a um regime de autorização prévia, o prestador deve disponibilizar a informação relativa à actividade que a concedeu. No caso de exercer uma profissão regulamentada, o prestador 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.

Por fim, assinale-se que, se implicarem custos para os destinatários além dos custos dos serviços de telecomunicações, incluindo ónus fiscais ou despesas de entrega, os serviços prestados devem ser objecto de informação clara anterior à sua utilização.

Aos elementos *supra* referidos acrescem, entre outros, quando o prestador de serviços em rede pretenda celebrar contratos em linha, os seguintes elementos, a ser facultados aos destinatários antes de ser dada qualquer ordem de encomenda:

- O processo de celebração do contrato;
- O arquivamento ou não do contrato pelo prestador de serviço e a acessibilidade àquele pelo destinatário;
- A língua ou as línguas em que o contrato pode ser celebrado;
- Os meios técnicos que o prestador disponibiliza para poderem ser identificados e corrigidos erros de introdução que possam estar contidos na ordem de encomenda;
- Os termos contratuais e as cláusulas gerais do contrato a celebrar;

- Os códigos de conduta de que seja subscritor e a forma de os consultar electronicamente.

Adverta-se que a não-disponibilização das informações previstas no parágrafo anterior constitui uma contra-ordenação punível com coima entre 2500 a 50 000 euros, agravada em um terço dos limites máximo e mínimo se o ilícito for praticado por uma pessoa colectiva [artigos 37.º, n.º 1, alínea *a*), e n.º 5 da LCE].

Por fim, resta referir que a exigência de informação dos elementos *supra* referidos pode ser afastada pelas partes, mediante acordo. Todavia, nas relações com consumidores, essa informação constitui um imperativo. Um consumidor não pode renunciar ao direito que lhe é conferido de obter os elementos de informação acima mencionados²³.

PROPOSTA CONTRATUAL, ORDEM DE ENCOMENDA E AVISO DE RECEPÇÃO

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, através do envio por este último da ordem de encomenda; caso contrário, estamos perante um mero convite a contratar, não ficando o prestador de serviços que emitiu o dito convite vinculado à celebração do contrato pela declaração da outra parte.

Logo que receba uma ordem de encomenda por via exclusivamente electrónica, o prestador de serviços deve acusar a recepção igualmente por meios electrónicos²⁴. O aviso de recepção constitui assim uma formalidade que visa assegurar ao destinatário a recepção da encomenda por parte do prestador de serviços²⁵. Este aviso de recepção deve conter a identificação fundamental do contrato a que se refere. Nos termos da LCE, considera-se que o prestador satisfaz o dever de acusar a recepção se enviar a comunicação para o endereço electrónico que foi indicado ou utilizado pelo destinatário do serviço.

Não obstante o que acima referimos, se ocorrer a imediata prestação em linha do produto ou serviço, a LCE dispensa o aviso de recepção.

Por fim, dispõe a LCE que a encomenda apenas se torna definitiva com a confirmação do destinatário, dada na sequência do aviso de recepção, reiterando a ordem emitida. Deste modo, o destinatário confirma a celebração do contrato, manifestando a sua vontade de que ele produza os seus efeitos naquele momento. Os efeitos do contrato ficam, pois, suspensos até à confirmação, que constitui uma condição

de eficácia daquele²⁶. Até que a confirmação suceda, o prestador de serviços não estará, ainda, obrigado a entregar a encomenda ou a prestar o serviço e o destinatário a efectuar a contraprestação.

Esclarece a LCE que a ordem de encomenda, o aviso de recepção e a confirmação da encomenda se consideram recebidos logo que os destinatários tenham a possibilidade de a eles aceder. Saliente-se que, no caso do correio electrónico, será suficiente a chegada da mensagem ao servidor do destinatário, não sendo necessária a sua recepção ou o conhecimento efectivo do seu conteúdo.

CONTRATAÇÃO SEM INTERVENÇÃO HUMANA

A LCE regula ainda os contratos celebrados entre computadores, sempre que as declarações negociais não sejam emitidas directamente com intervenção humana, estabelecendo que a esse tipo de contratação se aplica o regime geral aplicável à celebração de contratos, em que, além das normas constante do Código Civil, se incluem as normas acima enunciadas. Todavia, esse regime comum não se aplicará quando o regime jurídico dos contratos exigir uma actuação humana.

Designadamente, são aplicáveis as disposições sobre erro:

- na formação da vontade, se houver erro de programação;
- na declaração, se houver defeito de funcionamento da máquina;
- na transmissão, se a mensagem chegar deformada ao seu destino.

Assinale-se que a outra parte não pode opor-se à impugnação por erro sempre que lhe fosse exigível que dele se apercesse, nomeadamente pelo uso de dispositivos de detecção de erros de introdução. Dessa forma, recai sobre as partes de um contrato o ónus de detectar os erros constantes da declaração da outra parte que sejam exigíveis de ser apercebidos.

NOTAS

Pág. 8 ¹ LOUSA, Filipe José Viana (2003), *A Responsabilidade dos Prestadores de Serviços na Internet por Violações de Direito de Autor*. Lisboa, s. n., p. 23.

Pág. 8 ² ASCENSÃO, J. Oliveira (2003), «Contratação Electrónica», in AAVV, *Direito da Sociedade da Informação*, Coimbra, Coimbra Editora, vol. IV, p. 50.

Pág. 9 ³ LEITÃO, Luís Manuel Teles de Menezes (2002), «A Responsabilidade Civil na Internet», in AAVV, *Direito da Sociedade da Informação*, Coimbra, Coimbra Editora, vol. III, p. 156.

- Pág. 9 ⁴ Não se deve pois confundir o destinatário do serviço com o destinatário da transmissão, que será quem recebe a informação. Assim, por exemplo, quando se faz referência ao serviço de acesso à Internet, o *destinatário do serviço* será a pessoa que requer o serviço.
- Pág. 10 ⁵ PEREIRA, Alexandre Dias (2004), «Princípios do Comércio Electrónico», in AAVV, *Instituto de Direito das Empresas e do Trabalho. Miscelâneas n.º 3*, Coimbra, Livraria Almedina, p. 81.
- Pág. 10 ⁶ ASCENSÃO, José de Oliveira (2004), «Perspectiva Jurídica», in *O Comércio Electrónico em Portugal – O Quadro Legal e o Negócio*, Lisboa, ANACOM, p. 106.
- Pág. 10 ⁷ *Idem, ibidem*.
- Pág. 11 ⁸ PEREIRA, Alexandre Dias, *ob. cit.*, p. 85.
- Pág. 12 ⁹ LOUSA, Filipe José Viana, *ob. cit.*, p. 130.
- Pág. 14 ¹⁰ *Idem, ibidem*, p. 133.
- Pág. 15 ¹¹ A exigência de que o *caching* se restrinja a reproduções automáticas e temporárias significa que certos tipos de *caching*, que não constituem actividades temporárias nem automáticas, não beneficiarão desse regime. Em particular, não estará isenta de responsabilidade a actividade de *mirror caching* ou *mirroring*, que envolve uma armazenagem longa e deliberadamente efectuada por um prestador de serviços de um sítio da Internet.
- Pág. 15 ¹² Este requisito impede que se disponibilizem em *cache* sítios ou páginas da Internet que estejam submetidos a controlo de acesso mediante a utilização de palavras-chave sem esses mecanismos de controlo.
- Pág. 16 ¹³ O objectivo desta exigência é evitar que sítios ou páginas da Internet que obtenham os seus rendimentos a partir do número de visitas que recebem sejam prejudicadas pela prática do *caching*, que impediria de contabilizar, adequadamente, cada visita.
- Pág. 16 ¹⁴ Ministério da Justiça, Gabinete de Política Legislativa (2005), *Lei do Comércio Electrónico Anotada*, Coimbra, Coimbra Editora, p. 60.
- Pág. 17 ¹⁵ LOUSA, Filipe José Viana, *ob. cit.*, p. 140.
- Pág. 18 ¹⁶ *Idem, ibidem*.
- Pág. 21 ¹⁷ Ministério da Justiça, Gabinete de Política Legislativa, *ob. cit.*, p. 66.
- Pág. 23 ¹⁸ LE MEN, Yvon (s. d.), *Prática de Marketing Directo*, Porto, Rés Editora, p. 8.
- Pág. 23 ¹⁹ LINDON, Denis, LENDREVIE, Jacques *et al.* (2004), *Mercator XXI. Teoria e Prática do Marketing*, 10.^a ed., Lisboa, Publicações Dom Quixote, p. 642.
- Pág. 23 ²⁰ *Idem, ibidem*, p. 636.
- Pág. 23 ²¹ Ministério da Justiça, Gabinete de Política Legislativa, *ob. cit.*, p. 77.
- Pág. 24 ²² ROCHA, Manuel Lopes *et al.* (2004), *Guia do Comércio Electrónico*, Lisboa, Centro Atlântico, p. 62.
- Pág. 28 ²³ Ministério da Justiça, Gabinete de Política Legislativa, *ob. cit.*, p. 116.
- Pág. 28 ²⁴ Salvo acordo em contrário com a parte que não seja consumidora.
- Pág. 28 ²⁵ Ministério da Justiça, Gabinete de Política Legislativa, *ob. cit.*, p. 117.
- Pág. 29 ²⁶ *Idem, ibidem*, p. 118.

C A P Í T U L O

A Factura Electrónica

O B J E C T I V O S

- Dar a conhecer a evolução legislativa verificada desde a aprovação do primeiro diploma que aprovou e regulamentou o regime jurídico da factura electrónica até à actualidade, destacando o papel recente da Associação Aliança Digital (www.aliancadigital.pt)

Com a aprovação do Decreto-Lei n.º 357/99, de 18 de Setembro, que reconheceu e definiu o regime jurídico aplicável às facturas electrónicas, deu-se mais um passo no sentido da criação legislativa e regulamentar necessária ao desenvolvimento do comércio electrónico.

Já no ano de 1999, e sem prejuízo dos avanços pouco significativos que se verificaram durante a vigência do diploma referido, eram reconhecidos como objectivos essenciais nesta matéria a desmaterialização da factura e a introdução no ordenamento jurídico português do princípio da equiparação entre facturas emitidas em suporte papel e facturas electrónicas.

À luz do diploma, regulamentado pelo Decreto-Regulamentar n.º 16/2000, e porque o Decreto-Lei n.º 357/99 de 18 de Setembro tinha também uma vertente fiscal, os sujeitos passivos de relação fiscal que pretendessem utilizar o sistema de facturação electrónica deveriam solicitá-lo à Direcção-Geral dos Impostos.

Concedida que fosse a autorização, o requerente deveria declarar à Direcção-Geral dos Impostos o início de utilização do sistema de transmissão por via electrónica das facturas ou dos documentos equivalentes, sendo que, caso não se verificasse o início da utilização dentro do prazo de um ano, a autorização caducaria.

A LEI DA FACTURA ELECTRÓNICA

Na sequência da aprovação da Directiva Comunitária n.º 2001/115/CE, de 20 de Dezembro, e com a sua transposição para o ordenamento jurídico português pelo Decreto-Lei n.º 256/2003, de 21 de Outubro, foi revogada a legislação anteriormente publicada sobre a factura electrónica.

A Directiva n.º 2001/115/CE, que visa simplificar, modernizar e harmonizar as condições aplicáveis à facturação em matéria de imposto sobre o valor acrescentado, veio alterar a Directiva n.º 77/388/CEE, reconhecendo que o desenvolvimento do comércio electrónico requeria a criação de um enquadramento jurídico para a utilização da facturação electrónica que permitisse salvaguardar as possibilidades de controlo das administrações fiscais.

Através desse diploma comunitário pretendeu-se, de forma a assegurar um bom funcionamento e desenvolvimento do mercado interno, estabelecer, a nível comunitário, para efeitos de imposto sobre o valor acrescentado, uma lista harmonizada de referências obrigatórias nas facturas, bem como algumas regras comuns de recurso à facturação electrónica e à armazenagem electrónica das facturas, assim como à autofacturação e à subcontratação das operações de facturação.

A adopção da referida Directiva n.º 2001/115/CE, no plano comunitário, pretendeu simplificar, modernizar e harmonizar, em matéria de IVA, alguns aspectos relacionados com a obrigação de facturação.

Dos aspectos relacionados com essa obrigação de facturação e introduzidos pelo referido instrumento de regulamentação comunitário salientamos:

- a adopção de uma lista harmonizada de elementos que devem constar de forma obrigatória nas facturas emitidas pelos sujeitos passivos do imposto;
- o estabelecimento de regras específicas relativas à elaboração, ao arquivamento e conservação das facturas, incluindo a transmissão e conservação por meios electrónicos;
- a possibilidade de recurso, em certas condições, à «autofacturação», bem como à contratação de terceiros para a elaboração de facturas.

No que concerne concretamente à matéria da transmissão e da conservação das facturas por meios electrónicos, a possibilidade passou a ser consagrada no Código do Imposto sobre o Valor Acrescentado (CIVA), sendo previstos os princípios e as condições genéricas para a sua utilização.

Por sua vez, a regulamentação dos aspectos relacionados com o quadro legal relativo às especificações de natureza informática ou técnica terá sido remetida para regulamentação por legislação especial, verificando-se, no entanto, que a entrada em vigor, a 1 de Janeiro de 2004, do Decreto-Lei n.º 256/2003, de 21 de Outubro não ficou condicionada à respectiva regulamentação.

O CIVA foi aprovado pelo Decreto-Lei n.º 394-B/84, de 26 de Dezembro, sucessivamente alterado. O código regula, designadamente, a incidência real e pessoal do imposto, as isenções, o valor tributável, as taxas do imposto, a liquidação e o pagamento, as obrigações dos contribuintes (dentre as quais se destaca a obrigação de emitir uma factura ou um documento equivalente por cada trans-

missão de bens ou prestação de serviços, bem como pelos pagamentos que lhes sejam efectuados antes da data da transmissão de bens ou da prestação de serviços), os regimes especiais, a competência para a fiscalização, o dever de colaboração e as garantias dos contribuintes (das quais destacamos o recurso hierárquico, a reclamação graciosa e a impugnação judicial).

O Decreto-Lei n.º 375/99, de 18 de Julho, que, conforme referimos anteriormente, veio a ser revogado pelo Decreto-Lei n.º 256/2003, de 21 de Outubro (este último prevê, no seu artigo 6.º, expressamente a revogação do Decreto-Lei n.º 375/99, de 18 de Julho, e do Decreto Regulamentar n.º 16/2000), equiparava a factura emitida em suporte papel à factura electrónica. Somos hoje obrigados a constatar que o referido diploma revogado acabou por nunca ter aplicação, atribuindo-se o facto à obrigatoriedade de autorização prévia da Direcção-Geral dos Impostos.

O Decreto-Lei n.º 256/2003, de 21 de Outubro (que transpôs para o ordenamento jurídico português a Directiva n.º 2001/115/CE, do Conselho, de 20 de Dezembro, que, por sua vez, alterou a Directiva n.º 77/388/CEE, tendo em vista simplificar, modernizar e harmonizar as condições aplicáveis à facturação em matéria de imposto sobre o valor acrescentado), introduziu inúmeras alterações ao CIVA. Note-se que a referida Directiva n.º 77/388/CEE (a sexta directiva do IVA) do Conselho, de 17 de Maio, teve em vista a harmonização das legislações dos Estados-membros respeitantes aos impostos sobre o volume de negócios – sistema comum do imposto sobre o valor acrescentado: matéria colectável uniforme, tendo procedido à uniformização da base tributável do imposto a aplicar em todos os Estados-membros da CEE.

Dentre as alterações verificadas com a aprovação do Decreto-Lei n.º 256/2003, de 21 de Outubro, destacamos, designadamente, a alteração ao artigo 35.º do CIVA, que no seu n.º 10 estipula que as facturas ou os documentos equivalentes podem, sob reserva de aceitação pelo destinatário, ser emitidos por via electrónica, desde que seja garantida a autenticidade da sua origem e a integridade do seu conteúdo, mediante a aposição de assinatura electrónica avançada ou o uso de sistema de intercâmbio electrónico de dados (EDI).

Estabelece igualmente o citado diploma no seu artigo 7.º, no que concerne à condição de utilização do sistema, que até ao passado dia 31 de Dezembro de 2005, a utilização do sistema de transmissão de facturas ou documentos equivalentes por via electrónica estaria condicionada a prévia comunicação (e não já à autorização que vimos ser exigida à luz do Decreto-Lei n.º 375/99, de 18 de Julho) à DGI, não tendo tal comunicação efeitos suspensivos. Isso significa, claro está, que após aquela data, nem tão-pouco a formalidade de comunicação prévia é imposta ao sujeito passivo.

Recentemente, foi publicada a Resolução do Conselho de Ministros n.º 137/2005, que muitos consideram um passo verdadeiramente significativo na implementação da facturação electrónica no nosso país.

Não nos parece que a apreciação seja exagerada. Senão vejamos.

A resolução de 29 de Julho de 2005, publicada no *Diário da República* n.º 157, 1.ª série B, de 17 de Agosto de 2005, determina a adopção do sistema de facturação electrónica pelos serviços e organismos da administração pública. Considerou-se que, atendendo à importância do papel do Estado no domínio do comércio electrónico, era essencial determinar na administração pública, no caso de operações susceptíveis de processamento electrónico, a adopção do sistema de facturação electrónica e a preferência do Estado pela recepção das facturas correspondentes às operações realizadas enquanto adquirente de bens e serviços por via electrónica.

Por esses motivos, entre outros, determinou-se que, a partir de 1 de Janeiro de 2007, os serviços e organismos públicos integrados na administração directa e indirecta do Estado devem estar habilitados a emitir as facturas ou os documentos equivalentes por via electrónica, excepto se o destinatário solicitar o documento em papel. Para levar a cabo esse propósito, determinou-se que até 31 de Dezembro de 2006 essas entidades deverão adoptar os mecanismos necessários à emissão de facturas ou documentos equivalentes por via electrónica.

Na referida resolução foi igualmente estabelecido que a UMIC – Agência para a Sociedade do Conhecimento, IP – promoverá o acompanhamento e a avaliação da execução da referida resolução, informando regularmente o Governo da sua aplicação, tendo a UMIC a competência para receber dos serviços e organismos públicos integrados na administração directa e indirecta do Estado o calendário de aplicação das medidas a tomar para dar cumprimento à resolução, calendário esse que as entidades estão obrigadas a submeter no prazo máximo de seis meses.

Por último, e ainda em relação aos aspectos inovadores da resolução em análise e ao seu importante papel na implementação da facturação electrónica, destacamos a obrigatoriedade de os serviços e organismos públicos integrados na administração directa e indirecta do Estado comunicarem aos seus clientes e fornecedores a adopção do sistema de facturação electrónica e a sua preferência pela recepção de facturas ou documentos equivalentes por via electrónica com uma antecedência mínima de três meses relativamente ao seu início.

REQUISITOS LEGAIS

A Directiva n.º 2001/115/CE, de 20 de Dezembro, unificou as menções obrigatórias para efeitos de IVA que deverão constar em qualquer documento, analógico ou digital, para que possa ser designado como factura.

Os requisitos gerais da factura encontram-se previstos no artigo 35.º do CIVA, com a redacção introduzida pelo Decreto-Lei n.º 256-/2003, de 21 de Outubro.

No n.º 5 do citado artigo 35.º do Código do IVA exige-se que as facturas ou os documentos equivalentes sejam datados, numerados sequencialmente e contenham os elementos expressamente referidos nas várias alíneas do preceito:

«[...]»

As facturas ou documentos equivalentes devem ser datados, numerados sequencialmente e conter os seguintes elementos:

- a) Os nomes, firmas ou denominações sociais e a sede ou domicílio do fornecedor de bens ou prestador de serviços e do destinatário ou adquirente, bem como os correspondentes números de identificação fiscal dos sujeitos passivos de imposto;
- b) A quantidade e denominação usual dos bens transmitidos ou dos serviços prestados, com especificação dos elementos necessários à determinação da taxa aplicável; as embalagens não efectivamente transaccionadas deverão ser objecto de indicação separada e com menção expressa de que foi acordada a sua devolução;
- c) O preço, líquido de imposto, e os outros elementos incluídos no valor tributável;
- d) As taxas aplicáveis e o montante de imposto devido;
- e) O motivo justificativo da não aplicação do imposto, se for caso disso;
- f) A data em que os bens foram colocados à disposição do adquirente, em que os serviços foram realizados ou em que foram efectuados pagamentos anteriores à realização das operações, se essa data não coincidir com a da emissão da factura».

Para além desses elementos, que têm vindo a ser designados como requisitos gerais, a emissão de facturas electrónicas encontra-se igualmente sujeita a requisitos considerados específicos.

As facturas ou os documentos equivalentes podem, sob reserva de aceitação pelo destinatário, ser emitidos por via electrónica. A emissão de facturas electrónicas deverá ser *previamente* aceite pelo destinatário, assistindo-lhe o direito de reserva de aceitação que a facturação, a partir de um determinado momento, se processe por via electrónica (artigo 35.º, n.º 10, do Código do IVA).

Deverá ser garantida a autenticidade da sua origem e a integridade do seu conteúdo, mediante a aposição de assinatura electrónica avançada ou o uso de sistema de EDI – para efeitos de certeza e autenticidade (artigo 35.º, n.º 10, do CIVA).

Sempre que o registo das operações mencionadas nas alíneas b) e c) do n.º 2 do artigo 44.º do CIVA – «as importações de bens efectuadas pelo sujeito passivo e destinadas às necessidades da sua empresa» e «as transmissões de bens e prestações de serviços efectuadas ao sujeito passivo no quadro da sua actividade empresarial» –, referido no n.º 1 do artigo 48.º do mesmo diploma, respeite a facturas ou documentos equivalentes emitidos por via electrónica, deverão ser conservados em suporte papel listagens dessas facturas ou desses documentos equivalentes, por cada período de tributação, aplicando-se, com as necessárias adaptações, o disposto no artigo 48.º, n.º 2, do CIVA.

Embora o Decreto-Lei n.º 256/2003 não o tenha expressamente consagrado, as facturas e os documentos equivalentes transmitidos por meios electrónicos deverão ser conservados (durante o prazo legal de dez anos) num sistema que garanta a sua conservação sem alterações, por ordem cronológica de emissão e recepção.

Só é permitido o arquivamento em suporte electrónico das facturas ou dos documentos equivalentes emitidos por via electrónica se se garantir o acesso completo e em linha por parte da administração fiscal aos dados e se for assegurada a integridade da origem e do seu conteúdo (artigo 52.º, n.º 4, do CIVA).

Nos termos do disposto no artigo 5.º, n.º 5, do Decreto-Lei n.º 127-/90, de 17 de Abril, que transpõe para a ordem jurídica nacional a Directiva n.º 77/799/CEE do Conselho, de 19 de Dezembro, relativa à assistência mútua das autoridades competentes dos Estados-membros no domínio dos impostos directos, prevê-se que a autoridade competente portuguesa, ou seja, a DGI, tenha, dentro dos limites da regulamentação interna, direito ao acesso por via electrónica, ao carregamento e à utilização dos dados constantes das facturas emitidas ou recebidas por sujeitos passivos que disponham de sede, estabelecimento estável ou domicílio em território nacional, cujo arquivamento, efectuado através de meios electrónicos que garantam o acesso em linha aos dados, se verifique no território de outro Estado-membro.

«AUTOFACTURAÇÃO»

E EMISSÃO DE FACTURAS POR TERCEIROS

Pela Directiva n.º 2001/115/CE, passou a ser permitida, designadamente, a «autofacturação», a armazenagem de facturação em local

distinto da sede (nos termos analisados no ponto anterior) e a contração de terceiros para a elaboração das facturas.

No que concerne concretamente à autofacturação, será relevante atender ao facto de a elaboração de facturas ou documentos equivalentes por parte do adquirente dos bens ou serviços ficar sujeita à existência de um acordo prévio escrito entre o sujeito passivo transmitente e o adquirente, devendo o adquirente provar que o transmitente tomou conhecimento da emissão da factura e aceitou o seu conteúdo.

Tais faculdades poderão vir a originar a intervenção de terceiros, a vários níveis:

- licenciamento de soluções de facturação electrónica (*e-billing*); e/ou
- prestação de serviços de assistência técnica dessas soluções informáticas; e/ou
- prestação de serviços de emissão, custódia, armazenamento, entre outros, de facturas ou documentos equivalentes.

Na verdade, temos assistido nos últimos tempos ao aparecimento de vários fornecedores de soluções de factura electrónica, que oferecem igualmente aos seus clientes serviços de custódia de documentos electrónicos e um conjunto de serviços adicionais que visam facilitar as suas adesão e implementação ao processo de facturação electrónica.

Refere-se no artigo 52.º, n.º 3, do CIVA que os sujeitos passivos com sede, estabelecimento estável ou domicílio em território nacional são obrigados a manter os livros, registos e demais documentos referidos no n.º 1 do mesmo artigo – «todos os livros, registos e respectivos documentos de suporte, incluindo, quando a contabilidade é estabelecida por meios informáticos, os relativos à análise, programação e execução dos tratamentos» – em estabelecimento ou instalação situado em território nacional, salvo se o arquivamento for efectuado por meios electrónicos.

UTILIZAÇÃO DO EDI

Tal como referido anteriormente, os sistemas de facturação electrónica devem garantir a autenticidade da origem de cada factura ou documento equivalente, a integridade do conteúdo e da sequência e a validação cronológica das mensagens emitidas como facturas ou do-

cumentos equivalentes, o seu armazenamento em suporte informático, a manutenção da autenticidade, integridade e disponibilidade do conteúdo original das facturas e dos documentos equivalentes transmitidos por meios electrónicos, durante os prazos legalmente previstos, o não-repúdio da origem e a recepção das mensagens.

As facturas ou os documentos equivalentes podem, sob reserva de aceitação pelo destinatário, ser emitidos por via electrónica, desde que seja garantida a autenticidade da sua origem e a integridade do seu conteúdo, mediante a aposição de assinatura electrónica avançada ou o uso de sistema de intercâmbio electrónico de dados.

Existem duas formas de garantir a autenticidade da origem e a integridade do conteúdo de uma factura: através da utilização de uma assinatura electrónica avançada ou de um sistema de intercâmbio electrónico de dados.

A emissão das facturas ou dos documentos equivalentes poderá ocorrer por intercâmbio electrónico de dados, desde que a transferência electrónica seja suportada por uma mensagem de EDI, estruturada segundo um padrão previamente acordado entre o emissor e o receptor. O acordo prévio para intercâmbio electrónico de facturas ou documentos equivalentes deverá ser celebrado por escrito, entre o sujeito passivo transmissor dos bens ou prestador de serviços e o seu adquirente ou destinatário, designadamente no que diz respeito ao padrão de EDI adoptado, autenticidade da origem das mensagens, integridade do conteúdo, não-repúdio e protecção contra alterações.

A este respeito, o artigo 2.º, n.º 2, da Directiva n.º 2001/115/CE faz uma referência expressa ao intercâmbio electrónico de dados, nos termos definidos no artigo 2.º da Recomendação n.º 1994/820/CE da Comissão, de 19 de Outubro, relativa aos aspectos jurídicos da transferência electrónica de dados.

Através de um acordo de EDI, as partes podem convencionar que as facturas ou os documentos equivalentes relativos a qualquer transacção de bens ou serviços celebrada entre as partes passarão, a partir da data de assinatura do acordo, a ser emitidos através de intercâmbio electrónico de dados, sendo a transferência electrónica suportada por uma mensagem de EDI. A autenticidade da origem e a integridade do conteúdo das facturas electrónicas serão garantidas mediante mecanismos de autenticação de mensagens inerentes ao próprio padrão adoptado.

Ou seja, os aderentes vinculam-se a adoptar o EDI como meio de transmissão de mensagens uniformizadas que consubstanciem a formação das suas transacções negociais.

UTILIZAÇÃO DA «ASSINATURA ELECTRÓNICA AVANÇADA»

A garantia de autenticidade da origem e de integridade do conteúdo das facturas ou dos documentos equivalentes poderá ser assegurada mediante uma assinatura electrónica avançada, remetendo-se dessa forma para o regime jurídico dos documentos electrónicos e da assinatura digital (Decreto-Lei n.º 290-D/99, de 2 de Agosto, alterado pelo Decreto-Lei n.º 62/2003, de 3 de Abril).

A assinatura electrónica avançada é a assinatura electrónica que preenche os seguintes requisitos:

- i) Identifica «de forma unívoca o titular como autor do documento»;
- ii) A sua aposição ao documento depende «apenas da vontade do titular»;
- iii) É criada com meios que o titular pode manter sob seu controlo exclusivo;
- iv) A sua ligação ao documento permite «detectar toda e qualquer alteração superveniente do conteúdo deste» (artigo 2.º, alínea c), do Decreto-Lei n.º 290-D/99, de 2 de Agosto, com a redacção introduzida pelo Decreto-Lei n.º 62/2003, de 3 de Abril).

A assinatura electrónica avançada é definida no artigo 2.º, n.º 2, da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas electrónicas (disponível em http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=399L0093&model=guichett).

Na nova versão do Decreto-Lei n.º 290-D/99, de 2 de Agosto, alterado pelo Decreto-Lei n.º 62/2003, de 3 de Abril, são estabelecidas três modalidades de assinaturas electrónicas:

- «Assinatura electrónica: resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico»;
- Assinatura electrónica avançada (em que se inclui a assinatura digital): conforme referido acima, entende-se por assinatura electrónica avançada a assinatura electrónica que

preenche os seguintes requisitos: i) Identifica «de forma única o titular como autor do documento»; ii) «A sua aposição ao documento depende apenas da vontade do titular»; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua «conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste»; a assinatura digital é uma modalidade de assinatura electrónica avançada «baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura»;

- Assinatura electrónica qualificada: assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.

A ASSOCIAÇÃO ALIANÇA DIGITAL

Tal como se poderá constatar pela consulta do sítio da associação, em www.aliancadigital.pt, a Aliança Digital foi apresentada ao público no dia 12 de Julho de 2005, tendo desde essa data iniciado e desenvolvido um movimento em prol da dinamização e implantação da factura electrónica em Portugal.

O objectivo da associação, nas palavras dos seus fundadores, passa pela materialização, «num conjunto de políticas concretas de actuação, do vasto interesse demonstrado pelas empresas e pelo Estado em relação à Factura Electrónica», designadamente promovendo «sessões públicas com o objectivo de esclarecer, trocar experiências e recolher propostas para definição de *standards* e boas-práticas».

TESTE OS SEUS CONHECIMENTOS

1. É verdade que à luz do Decreto-Lei n.º 357/99, de 18 de Setembro, os sujeitos passivos de relação fiscal que pretendessem utilizar o sistema de facturação electrónica deveriam:

- a) pedir autorização à Direcção-Geral dos Impostos?
- b) apenas comunicar previamente essa intenção à Direcção-Geral dos Impostos?

2. De acordo com o Decreto-Lei n.º 256/2003, de 21 de Outubro, actualmente em vigor, as facturas ou os documentos equivalentes podem ser emitidos por via electrónica? Se sim, em que condições?

3. A elaboração de facturas ou documentos equivalentes por parte do adquirente dos bens ou dos serviços fica sujeita a que requisitos?

- a) à existência de um acordo prévio escrito entre o sujeito passivo transmitente e o adquirente;
- b) à existência de um acordo prévio escrito entre o sujeito passivo transmitente e o adquirente, devendo o adquirente provar que o transmitente tomou conhecimento da emissão da factura e aceitou o seu conteúdo; ou
- c) à existência de autorização prévia da Direcção-Geral dos Impostos?

Protecção de Dados Pessoais

O B J E C T I V O S

- Identificar as questões essenciais que são colocadas pela legislação portuguesa em matéria de protecção dos dados pessoais, elencando os passos que têm vindo a ser dados no sentido de clarificar a matéria da legalização dos tratamentos de dados pessoais e dos direitos, liberdades e garantias dos cidadãos

O advento e o desenvolvimento das tecnologias da informação têm vindo a colocar inúmeras questões em torno do direito à privacidade.

Tal como notam Ana Margarida Marques, Mafalda Anjos e Sónia Queiróz Vaz na obra 101 Perguntas e Respostas do Direito da Internet e da Informática: «Quando, em Junho de 1949, George Orwell escreveu o livro 1984, umas das mais emblemáticas obras de sempre da literatura que eternizou a figura do Big Brother, estava longe de imaginar que, o que na altura não passava de pura ficção, acabaria 50 anos mais tarde por se vir a concretizar na realidade. Ou quase. A verdade é que os avanços tecnológicos e as redes de comunicações que proliferaram pelo mundo na segunda metade do século, nomeadamente a Internet, determinaram o aparecimento de formas de vigilância e violação da privacidade dos cidadãos, princípio basilar do Estado de Direito».

No entanto, não poderá descurar-se a inevitabilidade de o Estado recolher e deter informação sobre os seus cidadãos que permita planificar e desenvolver a vida numa sociedade democrática.

O problema que aqui se coloca é identificado por Lourenço Martins Garcia Marques de forma bastante esquematizada: «Como compatibilizar o direito do indivíduo ao exercício das suas liberdades e ao gozo da sua intimidade com a necessidade do corpo social em que está integrado – e das entidades de direito público ou de direito privado com as quais vai estabelecendo relações jurídicas ao longo do tempo – de recolher informações jurídicas acerca de si, do seu passado e do seu presente?».

QUADRO DA LEGISLAÇÃO FUNDAMENTAL

A CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA

O artigo 35.º da Constituição da República Portuguesa estabelece, expressamente, no que concerne à utilização da informática:

«[...]»

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 rectificação e actualização, 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, co-

nexão, transmissão e utilização, e garante a sua protecção, 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 excepcionais 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 protecção 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 protecção idêntica à prevista nos números anteriores, nos termos da lei.

[...]».

Este normativo constitucional prevê o direito de protecção da privacidade face à utilização dos dados pessoais, tendo sido a Constituição Portuguesa, como nota Catarina Sarmiento e Castro na sua obra *Direito da Informática, Privacidade e Dados Pessoais*, «[...] a 1.^a Constituição Europeia a integrar um dispositivo especial em matéria de dados pessoais».

Para além desse aspecto, o artigo 35.º estabelece o direito de acesso aos dados informatizados que nos digam respeito, o direito de rectificação e de actualização e o direito de conhecer a finalidade a que se destinam, princípios esses que acabariam por ser vertidos na Lei de Protecção de Dados Pessoais (LPDP), que analisaremos à frente, aprovada pelo Lei 67/98, de 26 de Outubro.

O artigo citado da Constituição da República Portuguesa faz uma remissão no seu n.º 2 para a lei de definição dos conceitos de dados pessoais e das condições aplicáveis ao seu tratamento, transmissão e utilização, fazendo igualmente uma especial referência aos dados sensíveis (n.º 3), referência idêntica à adoptada posteriormente pela LPDP.

ALGUMAS DISPOSIÇÕES INTERNACIONAIS E EUROPEIAS

São vários os diplomas internacionais que incluem disposições sobre esta matéria, sendo de destacar, como faz Catarina Sarmento e Castro na obra supracitada, que «os principais documentos de Direito Internacional relativos à protecção dos Direitos do Homem ainda não contêm referências expressas à protecção de dados pessoais, muito embora já protejam expressamente a privacidade».

Tal como refere a autora, «a sua interpretação ao longo dos tempos acabou por dar guarida a esse aspecto particular». Ou seja, mesmo não se referindo expressamente à protecção de dados pessoais, as referidas disposições inseridas nos documentos de Direito internacional protegiam já a privacidade, sendo interpretadas no sentido de proteger aqueles dados (protecção genérica).

Assim, destacaríamos com relevância sobre esta matéria as seguintes disposições internacionais:

- Declaração Universal dos Direitos do Homem, artigo 12.º (disponível em <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/cidh-dudh.html>):

«[...]

Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.

[...]»;

- Pacto internacional relativo aos direitos civis e políticos, artigo 17.º (disponível em <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/cidh-dudh-direitos-civis.html>):

«[...]

1. Ninguém será objecto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.

2. Toda e qualquer pessoa tem direito à protecção da lei contra tais intervenções ou tais atentados.

[...]»;

- Convenção Europeia dos Direitos do Homem, artigo 8.º (disponível em <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhregionais/conv-tratados-04-11-950-ets-5.html>):

«[...]

(Direito ao respeito pela vida privada e familiar)

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

[...]»;

- Convenção 108 do Conselho da Europa, artigo 1.º (disponível em <http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>):

«A Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito (“protecção dos dados”)).».

Esta convenção já protege a privacidade do indivíduo na perspectiva do tratamento que pode ser dado a informações pessoais que lhe respeitem, tendo consagrado princípios que vieram a ser vertidos na Directiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro, relativa à protecção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Esta directiva comunitária viria a ser transposta para o ordenamento jurídico português pela LPDP (disponível em http://www.cnpd.pt/bin/legis/leis_nacional.htm).

Para além das disposições internacionais elencadas sobre esta matéria, foram adoptadas várias recomendações do Comité de Ministros do Conselho da Europa (para mais informações, consultar http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/).

O principal instrumento de regulação comunitária em sede de protecção de dados pessoais é a já mencionada Directiva n.º 95/46/CE do PE e do Conselho de 24 de Outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados (disponível em <http://www.cnpd.pt/bin/legis/internacional/95-46-CE.pdf>).

Muitos são os autores que designam esse diploma como o texto de referência, a nível europeu, em matéria de protecção de dados pessoais.

Para além do regime resultante dessa directiva, o tratamento de dados pessoais no sector específico das telecomunicações encontra-se regulado na Directiva n.º 97/66/CE, de 15 de Dezembro (disponível em <http://www.icp.pt/template20.jsp?categoryId=55050&contentId=87628>), transposta para o direito português pela Lei n.º 69/98, de 28 de Outubro, que regula o tratamento e a protecção de dados pessoais no sector das telecomunicações.

A Lei n.º 69/98, de 28 de Outubro, foi posteriormente revogada pela Lei n.º 41/2004, de 18 de Agosto (disponível em http://www.cnpd.pt/bin/legis/leis_nacional.htm), que transpõe a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas («Directiva relativa à privacidade e às comunicações electrónicas», disponível em <http://www.cnpd.pt/bin/legis/internacional/2002-58-CE-telecomunicações.pdf>).

A referida Directiva n.º 2002/58/CE regula aspectos respeitantes ao tratamento de dados pessoais no sector das comunicações electrónicas.

Refere-se, designadamente, às condições de segurança, à confidencialidade das comunicações, ao tratamento de dados de tráfego de comunicações, à facturação detalhada, à apresentação e restrição da identificação da linha chamadora e da linha ligada, ao reencaminhamento automático de chamadas, às listas de assinantes, e às comunicações não solicitadas (*spam*).

Note-se que, apesar de a transposição da n.º Directiva 2002/58/CE para a ordem jurídica nacional ter sido assegurada pela Lei n.º 41/2004, de 18 de Agosto, houve uma disposição da directiva que não foi transposta pelo referido diploma – o artigo 13.º –, referente a comunicações não solicitadas:

«[...]»

Artigo 13.º

Comunicações não solicitadas

1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de

aparelhos de fax ou de correio electrónico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio.

2. Sem prejuízo do n.º 1, se uma pessoa singular ou colectiva obtiver dos seus clientes coordenadas electrónicas de contacto para correio electrónico, no contexto da venda de um produto ou serviço, nos termos da Directiva 95/46/CE, essa pessoa singular ou colectiva poderá usar essas coordenadas electrónicas de contacto para fins de comercialização directa 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 electrónicas de contacto quando são recolhidos e por ocasião de cada mensagem, quando o cliente não tenha inicialmente recusado essa utilização.

3. Os Estados-Membros tomarão as medidas necessárias para assegurar que, por forma gratuita, não sejam permitidas comunicações não solicitadas para fins de comercialização directa em casos diferentes dos referidos nos n.ºs 1 e 2 sem o consentimento dos assinantes em questão ou que digam respeito a assinantes que não desejam receber essas comunicações, sendo a escolha entre estas opções determinada pela legislação nacional.

4. Em todas as circunstâncias, é proibida a prática do envio de correio electrónico para fins de comercialização directa, dissimulando ou escondendo a identidade da pessoa em nome da qual é efectuada a comunicação, ou sem um endereço válido para o qual o destinatário possa enviar um pedido para pôr termo a essas comunicações.

5. O disposto nos n.ºs 1 e 3 aplica-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 a comunicações não solicitadas.

[...]».

Na verdade, o artigo 1.º da Lei n.º 41/2004, de 18 de Agosto, relativa ao objecto e ao âmbito do diploma, estabelece que «a presente lei transpõe para a ordem jurídica nacional a Directiva 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 protecção da privacidade no sector das comunicações electrónicas, com excepção do seu artigo 13.º, referente a comunicações não solicitadas».

Essa situação ficou a dever-se ao facto de esse artigo em concreto ter já sido transposto para o ordenamento jurídico português pela conhecida Lei do Comércio Electrónico (Decreto-Lei n.º 7/2004, de 7 de Janeiro, disponível em <http://www.icp.pt/template20.jsp?categoryId=96804&contentId=149279>, que, no uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno – disponível em <http://www.icp.pt/template20.jsp?categoryId=63989&contentId=101352>).

Nesta medida, o Decreto-Lei n.º 7/2004, de 7 de Janeiro, representa a transposição parcial da Directiva n.º 2002/58/CE no que respeita ao artigo 13.º. A referida transposição foi assim assegurada pelo artigo 22.º do Decreto-Lei n.º 7/2004:

«[...]»

Artigo 22.º

Comunicações não solicitadas

1 – O envio de mensagens para fins de *marketing* directo, cuja recepção seja independente de intervenção do destinatário, nomeadamente por via de aparelhos de chamada automática, aparelhos de telecópia ou por correio electrónico, carece de consentimento prévio do destinatário.

2 – Exceptuam-se as mensagens enviadas a pessoas colectivas, ficando, no entanto, aberto aos destinatários o recurso ao sistema de opção negativa.

3 – É também permitido ao fornecedor de um produto ou serviço, no que respeita aos mesmos ou a produtos ou serviços análogos, enviar publicidade não solicitada aos clientes com quem celebrou anteriormente transacções, se ao cliente tiver sido explicitamente oferecida a possibilidade de o recusar por ocasião da transacção realizada e se não implicar para o destinatário dispêndio adicional ao custo do serviço de telecomunicações.

4 – Nos casos previstos nos números anteriores, o destinatário deve ter acesso a meios que lhe permitam a qualquer

momento recusar, sem ónus e independentemente de justa causa, o envio dessa publicidade para futuro.

5 – É proibido o envio de correio electrónico para fins de *marketing* directo, ocultando ou dissimulando a identidade da pessoa em nome de quem é efectuada a comunicação.

6 – Cada comunicação não solicitada deve indicar um endereço e um meio técnico electrónico, de fácil identificação e utilização, que permita ao destinatário do serviço recusar futuras comunicações.

7 – Às entidades que promovam o envio de comunicações publicitárias não solicitadas cuja recepção seja independente da intervenção do destinatário cabe manter, por si ou por organismos que as representem, uma lista actualizada de pessoas que manifestaram o desejo de não receber aquele tipo de comunicações.

8 – É proibido o envio de comunicações publicitárias por via electrónica às pessoas constantes das listas prescritas no número anterior».

De destacar, ainda relativamente a esta matéria, é a resolução legislativa do Parlamento Europeu sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva n.º 2002/58/CE [COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)]. A proposta de directiva foi aprovada a 14 de Dezembro de 2005.

Esta proposta de directiva aprovada pelo Parlamento obriga os operadores e os fornecedores de acesso à Internet a manterem os dados resultantes das comunicações efectuadas através das suas redes – incluindo as chamadas telefónicas falhadas – entre seis meses a dois anos.

As empresas da área das telecomunicações terão de facultar essa informação sempre que exista um pedido formal por parte das autoridades judiciais.

Verificaram-se já, por parte dos operadores, inúmeras reacções, que se prendem com os custos adicionais que o processo de retenção acarreta, sobretudo os relacionados com a disponibilização dos dados aos tribunais e aos órgãos de polícia criminal.

Não menos efusivas foram as reacções de associações cívicas que temem a existência de um verdadeiro *Big Brother* nas comunicações, salientando que todos os cidadãos da União Europeia serão controlados e monitorizados. As associações criticam ainda o facto de os pedi-

dos de informações das autoridades judiciais não serem limitados a determinados tipos de crimes. Ou seja, para essas associações, a gravidade de certos crimes, atendendo, designadamente, às medidas das penas abstractamente aplicáveis, pode justificar a disponibilização das informações, que já não se pode contudo justificar em crimes menos graves.

AS DISPOSIÇÕES JURÍDICAS NACIONAIS

No que concerne às disposições nacionais, temos vindo a fazer referência aos diplomas mais importantes.

Assim, a Lei n.º 67/98, de 26 de Outubro, já anteriormente designada como LPDP, transpõe para a ordem jurídica interna a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Por sua vez, a Lei n.º 41/2004, de 18 de Agosto transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, com excepção do seu artigo 13.º, referente a comunicações não solicitadas.

Também a Lei n.º 99/2003, de 27 de Agosto, que aprovou o Código do Trabalho, introduziu relevantes disposições relativas à protecção dos dados pessoais. Senão vejamos:

«[...]»

Artigo 17.º

Protecção de dados pessoais

1 – O empregador não pode exigir ao candidato a emprego ou ao trabalhador que preste informações relativas à sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar a respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação.

2 – O empregador não pode exigir ao candidato a emprego ou ao trabalhador que preste informações relativas à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação.

3 – As informações previstas no número anterior são prestadas a médico, que só pode comunicar ao empregador se

o trabalhador está ou não apto a desempenhar a actividade, salvo autorização escrita deste.

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

5 – 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 protecção de dados pessoais.

[...]

Artigo 19.º

Testes e exames médicos

1 – Para além das situações previstas na legislação relativa a segurança, higiene e saúde no trabalho, o empregador não pode, para efeitos de admissão ou permanência no emprego, exigir ao candidato a emprego ou ao 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 protecção e segurança do trabalhador ou de terceiros, ou quando particulares exigências inerentes à actividade o justifiquem, devendo em qualquer caso ser fornecida por escrito ao candidato a emprego ou trabalhador a respectiva fundamentação.

2 – O empregador não pode, em circunstância alguma, exigir à candidata a emprego ou à 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 actividade, salvo autorização escrita deste.

[...]

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 do equipamento identificado no número anterior é lícita sempre que tenha por finalidade a protecção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem.

3 – Nos casos previstos no número anterior o empregador deve informar o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados.

[...]

Artigo 21.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 electrónico.

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 electrónico.

[...]».

Também a Lei n.º 35/2004, de 29 de Julho, que regulamenta a Lei n.º 99/2003, de 27 de Agosto, que aprovou o Código do Trabalho, estabelece disposições importantes em sede de protecção de dados pessoais, destacando-se as seguintes:

«[...]»

Capítulo IV

Direitos de personalidade

Artigo 27.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 objectivos a atingir.

3 – Os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tra-

tamento 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, 10 dias após a consulta, comprovativo do pedido de parecer.

Artigo 28.º

Utilização de meios de vigilância a distância

1 – Para efeitos do n.º 2 do artigo 20.º do Código do Trabalho, 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 referida no número anterior só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objectivos 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, 10 dias após a consulta, comprovativo do pedido de parecer.

Artigo 29.º

Informação sobre meios de vigilância a distância

Para efeitos do n.º 3 do artigo 20.º do Código do Trabalho, o empregador deve afixar nos locais de trabalho em que existam meios de vigilância a distância 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».

A 30 de Setembro de 2005, o Conselho de Ministros adoptou a Resolução n.º 154/2005, que adopta medidas com vista ao desenvolvimento do passaporte electrónico português (PEP).

Entre outras medidas, o Conselho de Ministros resolveu, no âmbito dessa iniciativa legislativa, aprovar as opções fundamentais do

projecto de emissão do novo passaporte electrónico português, constantes de documento anexo, nos termos decorrentes do Regulamento (CE) 2252/2004, do Conselho, de 13 de Dezembro, reforçar os meios de coordenação e preparação do projecto nas suas componentes legal, orgânica e operacional e determinar que, para tal fim e sob coordenação do Ministério da Administração Interna, sejam tomadas, com a máxima urgência, as medidas necessárias para fixar definitivamente todas as componentes do modelo, incluindo as referentes ao modo de captação de dados, aos equipamentos de leitura a utilizar, os procedimentos a adoptar pelos serviços envolvidos e os sistemas de comunicações.

Mais recentemente, foi aprovado o Decreto-Lei n.º 207/2005, de 29 de Novembro, que visa regular o regime especial autorizado pelo artigo 13.º da Lei n.º 1/2005, de 10 de Janeiro, na redacção decorrente da Lei n.º 39-A/2005, de 29 de Julho, definindo:

- a) Os procedimentos a adoptar na instalação, pelas forças de segurança, de sistemas de vigilância electrónica rodoviária;
- b) As formas e condições de utilização pelas forças de segurança dos sistemas de vigilância rodoviária instalados ou a instalar pela Estradas de Portugal, EPE, e pelas empresas concessionárias rodoviárias nas respectivas vias concessionadas;
- c) Os procedimentos a adoptar para o tratamento da informação recolhida e o registo eficaz de acidentes, infracções ou quaisquer ilícitos;
- d) As formas através das quais as forças de segurança se coordenam para a interacção eficaz com as empresas, cujos equipamentos estão legalmente autorizadas a utilizar.

ALGUMAS NOÇÕES ESSENCIAIS

Para facilitar a compreensão do regime jurídico da protecção de dados pessoais, é essencial que se considerem determinados conceitos fundamentais sobre a matéria. Parece-nos absolutamente essencial para a compreensão deste regime que se saiba previamente o que são os dados pessoais ou que actividades ou actos são legalmente configuráveis como um tratamento desses dados.

DADOS PESSOAIS

Nos termos do seu artigo 4.º, a LPDP 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».

A LPDP «não se aplica ao tratamento de dados pessoais efectuado por pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas».

A LPDP «aplica-se ao tratamento de dados pessoais efectuado:

- a) No âmbito das actividades 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». Neste caso, «o responsável pelo tratamento deve designar, mediante comunicação à Comissão Nacional de Protecção 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».

A LPDP aplica-se igualmente 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». O disposto «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».

A LPDP «aplica-se ao tratamento de dados pessoais que tenham por objectivo 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 respectivos sectores».

Esta lei define, no seu artigo 3.º, dados pessoais como «qualquer informação, de qualquer natureza e independentemente do respectivo

suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (“titular dos dados”)); mais refere que «é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, 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».

É considerada identificável a pessoa que possa ser identificada directa ou indirectamente, ainda que por recursos a meios de que disponha um terceiro.

A esse respeito e, tal como refere Catarina Sarmento e Castro na página 71 da obra supracitada, o Tribunal de Justiça das Comunidades já se pronunciou sobre a interpretação da noção de dados pessoais – Acórdão de 6 de Novembro de 2003 – tendo concluído que o referido conceito «abrange, seguramente, o nome de uma pessoa a par do seu contacto telefónico ou de informações relativas às suas condições de trabalho ou aos seus passatempos».

Um dos exemplos referidos pela autora como dados que não são pessoais são os dados que não permitem identificar uma pessoa, isto mesmo que sejam dados que, em abstracto, se referem a pessoas. Como exemplo, a autora refere o caso dos dados estatísticos, que não permitem saber a que pessoas é que se referiam.

A CNPD teve já oportunidade de se pronunciar sobre os termos admissíveis de tratamento de vários tipos de dados pessoais. Através de várias orientações disponíveis em <http://www.cnpd.pt/bin/orientacoes/orientacoes.htm>, esta entidade administrativa definiu princípios orientadores relativos, designadamente, ao tratamento de dados por videovigilância, de dados biométricos para controlos de acesso e de assiduidade, e sobre a privacidade no local de trabalho: o controlo do correio electrónico, dos acessos à Internet e das chamadas telefónicas dos trabalhadores.

TRATAMENTO DE DADOS PESSOAIS

Outro conceito que surge como essencial para compreender o regime jurídico aplicável aos dados pessoais prende-se com o conceito de tratamento de dados. Ou seja, que actividades é que, sendo levadas a cabo, configuram verdadeiros tratamentos para efeitos de aplicação das leis de protecção de dados pessoais.

A própria LPDP, mais uma vez, adianta uma definição. No artigo 2.º, alínea *b*), estabelece-se que «“tratamento de dados pessoais” (“tratamento”) é qualquer operação ou conjunto de operações sobre dados

pessoais, efectuadas 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».

Tal como resulta da lei, não é apenas o registo de dados pessoais que constitui um tratamento de dados pessoais e esse aspecto assume uma importância inquestionável. Note-se, aliás, que mesmo as actividades que a LPDP elenca como constituindo um tratamento («a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a re-

cuperação, 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») são meramente exemplificativas, como atenta a expressão «tais como», que precede esse elenco. Assume a utilização dessa expressão a intenção de apresentar uma lista não exaustiva de actos, pelo que também outros podem configurar um tratamento de dados pessoais, ainda que a lei não os tenha expressamente previsto.

A este respeito, o Tribunal de Justiça das Comunidades Europeias, no acórdão supracitado de 6 de Novembro, pronunciando-se sobre o conceito de tratamento de dados pessoais, considerou que «a operação que consiste na referência, numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui “um tratamento de dados pessoais [...]”».

O TRATAMENTO DE DADOS PESSOAIS: CONDIÇÕES DE LEGITIMIDADE

A OBRIGAÇÃO DE NOTIFICAÇÃO DO TRATAMENTO, AS ISENÇÕES DE NOTIFICAÇÃO E O CONTROLO PRÉVIO DA CNPD (AUTORIZAÇÃO)

A obrigação de notificação do tratamento

A LPDP enuncia princípios fundamentais relativos à possibilidade de tratamento de dados pessoais. Um desses princípios consta do artigo 27.º (obrigação de notificação à CNPD), em que se prevê que «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» (sublinhado nosso).

O responsável pelo tratamento ou o seu representante deve notificar a CNPD através de formulário próprio disponível em www.cnpd.pt antes da realização de um tratamento.

As isenções de notificação

No entanto, no n.º 2 do mesmo artigo 27.º, a LPDP prevê a possibilidade de, em certos casos e cumpridas que sejam determinadas condições, não ser necessário o cumprimento dessa formalidade de notificação prévia.

Assim, «a CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, atendendo aos dados a tratar, não sejam susceptíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência» (sublinhado nosso).

Apresentamos ainda os artigos 3.º – «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» – e 4.º – «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».

Ou seja, «a CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos» (artigo 27.º, sublinhado nosso) quando considere que não são «susceptíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência». Há, portanto, excepções previstas, como autorizações da CNPD de isenção de notificação, que se encontram disponíveis para consulta em <http://www.cnpd.pt/bin/legal/isencoes.htm>.

A CNPD «decidiu isentar de notificação à Comissão alguns tratamentos de dados pessoais com finalidades específicas, desde que respeitadas determinadas condições», mantendo os responsáveis pelos tratamentos dos dados pessoais abrangidos por essas isenções as obri-

gações de (i) proceder ao tratamento dos dados pessoais estritamente dentro dos limites estabelecidos pela CNPD nas suas autorizações de isenção, publicadas em *Diário da República*; (ii) respeitar sempre o direito à informação, legalmente reconhecido ao titular dos dados, bem como o direito de acesso, rectificação, oposição e eliminação; e (iii) cumprir os princípios de protecção de dados de lealdade, licitude, legitimidade e pertinência no tratamento dos dados.

As referidas autorizações de isenção decididas pela CNPD foram, nos termos legalmente exigidos, publicadas no *Diário da República* n.º 22, 2.ª série, de 27 de Janeiro de 2000, na Deliberação 60/2000 e tiveram em vista: o processamento de retribuições, prestações, abonos de funcionários ou empregados (autorização de isenção n.º 1/99), a gestão de utentes de bibliotecas e arquivos (autorização de isenção n.º 2/99), a facturação e gestão de contactos com clientes, fornecedores e prestadores de serviços (autorização de isenção n.º 3/99), a gestão administrativa de funcionários, empregados e prestadores de serviços (autorização de isenção n.º 4/99), o registo de entradas e saídas de pessoas em edifícios (autorização de isenção n.º 5/99) e a cobrança de quotizações em associações e contactos com os respectivos associados (autorização de isenção n.º 6/99).

O controlo prévio da CNPD (a autorização)

Para além dessas situações de excepção ao princípio geral da obrigatoriedade de notificação prévia à CNPD dos tratamentos de dados pessoais, em que podemos dizer que se verifica uma exigência de formalidade, diríamos, *inferior* à que se verifica no caso da notificação, também existem situações em que essa formalidade não é suficiente, sendo requerida *a autorização da CNPD*.

Assim, nos termos do artigo 28.º da LPDP (Controlo prévio) carecem de autorização da CNPD: 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 da LPDP (respectivamente, os dados sensíveis e os dados pessoais relativos a «suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias»), o tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares, a interconexão de dados pessoais prevista no artigo 9.º da LPDP, a utilização de dados pessoais para fins não determinantes da recolha. Note-se que estes tratamentos previstos no n.º 1 do artigo 28.º podem ser autorizados por diploma legal, não carecendo nesse caso de autorização da CNPD.

São estes, portanto, os casos em que a formalidade exigida e que permitirá legitimar o tratamento dos dados pessoais em causa é considerada *superior*, exigindo-se uma verdadeira autorização da CNPD, não sendo suficiente perante a lei a mera formalidade da notificação prévia ao tratamento.

OS FUNDAMENTOS DO TRATAMENTO

De acordo com a LPDP, os tratamentos de dados pessoais, nos termos analisados anteriormente, só poderão ser efectuados se se verificar uma das condições de legitimidade ou um dos fundamentos legalmente previstos.

Ou seja, de uma maneira geral, o tratamento de dados pessoais não é admitido, a menos que, no caso concreto, se verifique pelo menos umas das condições legitimantes que fundamente esse tratamento que se encontram expressamente previstas no artigo 6.º da LPDP.

Assim, o tratamento de dados pessoais só pode ser efectuado se:

- (i) o seu titular tiver dado de forma inequívoca o seu consentimento ou
- (ii) se o tratamento for necessário para:

- a) «Execução de contrato ou contratos em que o titular dos direitos seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido.» Esta condição de legitimidade encontrar-se-á preenchida, por exemplo, aquando da recolha de dados para abertura de uma conta junto de uma instituição bancária, reserva de um bilhete de avião, solicitação de um cartão de crédito de um estabelecimento comercial (por exemplo, Jumbo, El Corte Inglés), entre muitos outros casos;
- b) «Cumprimento de obrigação legal a que o responsável do tratamento esteja sujeito.» Um exemplo desta condição de legitimidade do tratamento de dados verifica-se no direito do trabalho, mais concretamente no caso das obrigações de comunicação de dados pela entidade patronal a outras entidades públicas para fins fiscais ou relativos à segurança social;
- c) «Protecção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento.» Esta condição de legitimidade verificar-se-á nos casos de tratamento de dados de saúde realizado por estabelecimentos de saúde em estados de coma, de inconsciência, quando esteja envolvido um menor e não haja tempo de contactar o seu representante;

- d) «Execução de 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.» Catarina Sarmento e Castro apresenta como exemplo da verificação desta condição de legitimidade (na página 211 da sua obra supracitada) a situação prevista pela CNPD no Parecer n.º 22/2001, quando se refere que «quando um serviço público, no exercício das suas funções, necessite de contactar com um cidadão para realização de um interesse público relevante, interesse esse que se reflecta de forma positiva na esfera do particular e reunidas que estejam outras condições mencionadas no Parecer, será possível a comunicação do dado morada constante da Base de Dados do Recenseamento Eleitoral. Seria o caso do pedido de comunicação por parte do Centro Nacional de Pensões, quando pretenda obter morada do ascendente que tem a pessoa a cargo, para lhe atribuir uma pensão».
- e) Prossecução de interesses legítimos do responsável ou de terceiro a quem os dados sejam comunicados (desde que não devam prevalecer os interesses ou direitos do titular dos dados). Catarina Sarmento e Castro refere como exemplo da verificação desta condição legitimante a situação enunciada no mesmo Parecer da CNPD, n.º 22/2001, relativo à comunicação do dado «morada», designadamente ao Fundo de Garantia Automóvel, atendendo à sua sub-rogação nos direitos do lesado, após a satisfação da indemnização ao mesmo, decorrente de acidente originado por veículos sujeitos a seguro obrigatório.

OS DADOS PESSOAIS SENSÍVEIS

Os artigos 7.º, 8.º e 28.º da LPDP apresentam algumas das disposições mais importantes relativas às condições de tratamento de uma categoria particular de dados pessoais: os dados sensíveis.

Tal como vimos anteriormente, esses dados são aqueles cujo tratamento se encontra sujeito ao controlo prévio da CNPD.

Mas quais são, afinal, os dados pessoais considerados sensíveis?

São os 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 e os dados relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias.

Quanto estivermos em presença desses dados, não basta notificar a CNPD para que se possa proceder ao tratamento. É legalmente exigida no artigo 28.º, conforme referido anteriormente, uma autorização efectiva pela CNPD, no âmbito da qual essa entidade administrativa definirá os termos em que o tratamento é autorizado, após uma análise detalhada das condições em que o responsável do tratamento prevê que ele seja processado.

OS DIREITOS DOS TITULARES DOS DADOS

Os direitos dos titulares dos dados são os seguintes:

- Direito de informação – o responsável pelo tratamento deve informar o titular dos dados acerca da sua identidade, das finalidades do tratamento, dos destinatários dos dados, se é obrigatória ou facultativa a resposta ou o fornecimento de dados e as consequências se não responder, condições de exercício do direito de acesso e rectificação;
- Direito de acesso para ver e conhecer os dados;
- Direito de rectificação e actualização;
- Direito de apagamento ou bloqueio dos dados em caso de tratamento inexacto ou fora do prazo.

A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

TRANSFERÊNCIAS DENTRO DA UNIÃO EUROPEIA

O princípio da liberdade de transferência de dados pessoais na União Europeia significa que a circulação de dados pessoais entre Estados-membros da UE é livre.

TRANSFERÊNCIAS PARA UM ESTADO QUE NÃO PERTENÇA À UNIÃO EUROPEIA

Nesses casos, será necessário respeitar a Lei da Protecção de Dados Pessoais, sendo a transferência possível se o Estado para onde são transferidos os dados assegurar um nível de protecção adequado.

Note-se que «cabe à CNPD decidir se um Estado que não pertença à EU assegura um nível de protecção adequado» (artigo 19.º, n.º 3). Como decidirá a CNPD esta questão? Apreciando todas as circunstâncias da transferência: natureza dos dados, finalidade, duração, países de origem e de destino, regras de direito em vigor nesse Estado, regras profissionais e medidas de segurança aí respeitadas.

TRANSFERÊNCIAS PARA UM ESTADO QUE NÃO ASSEGURE UM NÍVEL DE PROTECÇÃO ADEQUADO

Esse tipo de transferências pode ser permitido pela CNPD (sem controlo prévio) nos termos do artigo 20.º, n.º 1, se o titular dos dados der de forma inequívoca o seu consentimento ou se a transferência:

- 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;
- 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;
- for necessária ou legalmente exigida para a protecção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial;
- for necessária para proteger os interesses vitais do titular dos dados; ou
- 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.

Esse tipo de transferências pode ainda ser permitido se forem dadas garantias pelo responsável de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas *mediante cláusulas contratuais adequadas* (exemplo: Decisão da Comissão, de 27 de Dezembro de 2001, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros).

TRANSFERÊNCIAS REALIZADAS AO ABRIGO DE CLÁUSULAS CONTRATUAIS-TIPO APROVADAS PELA COMISSÃO EUROPEIA

Essas transferências não são objecto de autorização da CNPD, que se limita a verificar a conformidade da transferência com tais cláusulas. São exemplos casos como os seguintes: Decisão da Comissão de 26 de Julho de 2000, relativa ao nível de protecção adequado assegurado pelos princípios «Safe Harbor»; Decisão da Comissão de 20 de Dezembro de 2001, relativa ao nível de protecção adequado assegurado pela lei canadiana; Decisão da Comissão de 30 de Junho de 2003, relativa ao nível de protecção adequado assegurado na Argentina.

SEGURANÇA E CONFIDENCIALIDADE DO TRATAMENTO DE DADOS PESSOAIS

A nossa lei defende que o responsável pelo tratamento de dados pessoais deve adoptar «medidas técnicas e organizativas adequadas para protecção dos dados pessoais, designadamente contra a destruição, a perda, a alteração, a difusão ou o acesso não autorizados».

Os responsáveis do tratamento e todos aqueles que no exercício das suas funções tenham conhecimento dos dados pessoais tratados ficam obrigados a sigilo profissional, mesmo após o termo das funções.

PRINCÍPIOS SUBJACENTES AO TRATAMENTO DE DADOS PESSOAIS

- Princípio da transparência – Deve ser dado a conhecer ao titular dos dados o tratamento, indicando-se os seus fins, sua duração e categorias de dados tratados.

- Princípio da finalidade – Os dados só podem ser utilizados para a finalidade determinante da recolha.
- Princípio da licitude e lealdade – Cumprimento da legislação aplicável e transparência
- Princípio da adequação, pertinência e proporcionalidade
- Princípio da exactidão e actualização

A TUTELA DOS DADOS PESSOAIS

A lei portuguesa prevê uma tutela administrativa e jurisdicional dos dados pessoais. Sem prejuízo do direito de apresentação de queixa à CNPD, qualquer pessoa pode recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento da legislação nesta área.

Se alguém sofreu um prejuízo por tratamento ilícito de dados, pode obter a sua reparação do responsável pelo tratamento (responsabilidade civil).

A tutela contra-ordenacional legalmente prevista nesta matéria traduz-se na previsão de coimas, por exemplo, quando não se notifica a CNPD, não se cumprem o direito à informação e as medidas especiais de segurança, entre outros casos.

Por último, os dados pessoais são também penalmente tutelados, sendo acções como o acesso indevido, a viciação ou destruição de dados pessoais ou a violação do dever de sigilo tipificados como crime e puníveis com penas de prisão ou multa.

TESTE OS SEUS CONHECIMENTOS

1. Qual das seguintes afirmações é incorrecta?
 - a) O consentimento do titular de dados pessoais é suficiente para o tratamento dos dados, não sendo exigida por lei, nesse caso, nenhuma outra formalidade prévia;
 - b) A imagem e a voz de uma pessoa são consideradas dados pessoais, para efeitos da lei;
 - c) O processamento de dados pessoais sensíveis só pode ser efectuado mediante autorização prévia da Comissão Nacional de Protecção de Dados;
 - d) A consulta de dados pessoais é considerada uma operação de tratamento de dados pessoais.

A Assinatura Electrónica

O B J E C T I V O S

- Dar a conhecer a evolução legislativa verificada desde a aprovação do primeiro diploma que aprovou o regime jurídico aplicável aos documentos electrónicos e assinatura digital até à actualidade



«A divulgação da Internet e de outras redes de comunicações públicas coloca aos respectivos utentes problemas delicados de confidencialidade dos dados trocados e de garantia de identidades dos intervenientes na comunicação.» (LOPES ROCHA, Manuel et al., Leis do Comércio Electrónico, Coimbra, Coimbra Editora, 2001)

ENQUADRAMENTO LEGISLATIVO

A assinatura e a factura electrónicas são documentos electrónicos ou meios de garantia previstos na lei, em especial no que diz respeito ao comércio electrónico.

A validade, a eficácia e o valor probatório dos documentos electrónicos e da assinatura digital são questões regulamentadas em Portugal pelo Decreto-Lei n.º 290-D/99, de 2 de Agosto. Tal como referem Manuel Lopes Rocha *et al.* na obra supracitada, o diploma surgiu na ordem jurídica portuguesa antes da aprovação e publicação da Directiva n.º 1999/93/CE, relativa a um quadro legal sobre assinaturas electrónicas, apesar de as versões preparatórias da directiva terem sido consideradas aquando da preparação do decreto-lei (Cfr. ob. cit., página 18).

O Decreto-Lei n.º 62/2003, de 3 de Abril, veio a transpor essa directiva, tendo alterado algumas disposições do Decreto-Lei n.º 290-D/99. O Decreto-Lei n.º 62/2003 regula a validade, a eficácia e o valor probatório dos documentos electrónicos, a assinatura electrónica e a actividade de certificação de entidades certificadoras estabelecidas em Portugal.

Mais recentemente, foi aprovada a Resolução do Conselho de Ministros n.º 171/2005, de 6 de Outubro, pela qual foi aprovada a criação da Entidade de Certificação Electrónica do Estado – Infra-Estrutura de Chaves Públicas (ECEE), sendo igualmente determinados os objectivos a assegurar pelo respectivo processo de instalação.

A aprovação da criação desta entidade decorreu da implementação de alguns programas públicos que visaram a promoção das tecnologias de informação e comunicação.

Através do Decreto-Lei n.º 116-A/2006, de 16 de Junho, foi criado o Sistema de Certificação Electrónica do Estado – Infra-Estrutura de Chaves Públicas.

A NOÇÃO LEGAL DE DOCUMENTO ELECTRÓNICO

A noção legal de documento electrónico é-nos fornecida pelo artigo 2.º do Decreto-Lei n.º 290-D/99 (regime jurídico dos documentos electrónicos e da assinatura electrónica), alterado pelo Decreto-Lei n.º 62/2003. O documento electrónico é definido como todo o documento elaborado mediante processamento electrónico de dados, ou seja, o «documento formado mediante o uso de equipamento informático, *maxime*, o computador».

Os documentos electrónicos são:

- em sentido estrito, os memorizados em forma digital em memórias magnéticas ou ópticas e destinados apenas a ser lidos pelo computador, pelo que não podem ser lidos e apercebidos pelo homem; e
- em sentido amplo (documentos informáticos), os gerados através de periféricos do computador.

VALOR PROBATÓRIO

O documento electrónico cujo conteúdo seja susceptível de representação escrita é havido, para todos os efeitos, como documento escrito e nos termos do artigo 26.º, n.º 1, do Decreto-Lei n.º 7/2004. As declarações por via electrónica satisfazem a exigência legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação.

A eficácia jurídica de um documento depende portanto de dois factores essenciais: genuinidade e segurança.

Em termos de genuinidade e segurança do documento electrónico, colocam-se três ordens de questões:

- Autenticidade – o problema da correspondência autor aparente/autor real, que se resolve com a aposição de assinatura;
- Integridade do documento – tem sido defendido que o problema se resolve com a inserção em arquivos protegidos;
- Confidencialidade – o problema poderá resolver-se com o recurso a técnicas de criptografia.

Em relação à questão da assinatura do documento electrónico, dado que ele não comporta a assinatura autógrafa, têm de ser utilizados outros meios de autenticação (assinatura electrónica, *lato sensu*), dos quais se têm vindo a destacar os códigos secretos, a assinatura digitalizada, a chave biométrica, a assinatura digital com criptografia simétrica com chave única e a assinatura digital com criptografia assimétrica com chave pública.

Entende-se por assinatura electrónica (*stricto sensu*), nos termos da directiva e da nossa legislação: «o resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico».

Na redacção original do Decreto-Lei n.º 290-D/99 só era aceite a autenticação legal dos documentos com a aposição de assinatura digital,

definida como «o processo de assinatura electrónica baseado num sistema criptográfico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo, e ao declaratório usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura».

A chave privada é o «elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se põe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública».

A chave pública é o «elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves».

A definição de assinatura digital não foi eliminada no Decreto-Lei n.º 62/2003, limitando-se o legislador a acrescentar um novo conceito: o de assinatura electrónica qualificada, que definiu como «*assinatura digital ou outra modalidade de assinatura electrónica avançada* que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura» (sublinhado nosso), uma definição mais ampla do que a de assinatura digital.

Coloca-se a seguinte questão: na assinatura electrónica avançada qualificada cabem as modalidades de assinatura electrónica *lato sensu*?

O que se tem defendido é que a resposta é globalmente negativa. Senão vejamos.

Os códigos secretos não identificam inequivocamente o autor do documento, não são apostos a este, e nem permitem detectar eventuais alterações.

Por sua vez, a assinatura digitalizada é copiada de um ficheiro, sendo que a sua aposição não depende apenas da vontade do seu titular e não permite detectar alterações posteriores do documento.

No que diz respeito às chaves biométricas, são meros meios de acessos a sistemas.

A assinatura digital de criptografia simétrica – chave única, por seu turno, não transmite a certeza de quem foi o autor do documento em causa (se o titular, se outra pessoa a quem foi fornecida a chave com o objectivo primário de verificar a assinatura do outro).

Estes aspectos têm permitido concluir que o sistema legal, apesar da confusão criada pelo legislador, continua a ser o sistema de criptografia assimétrica de chave pública.

A CERTIFICAÇÃO DA ASSINATURA

O valor da assinatura digital depende de o seu titular possuir um certificado digital válido emitido por uma entidade certificadora devidamente credenciada por um organismo competente (a autoridade credenciadora).

A autoridade credenciadora é a entidade competente para a credenciação e fiscalização das entidades certificadoras. Em Portugal, é o ITIJ – Instituto da Tecnologia de Informações na Justiça.

A entidade certificadora é, por sua vez, a entidade ou pessoa singular ou colectiva credenciada que cria ou fornece meios para a criação das chaves, emite os certificados de assinatura, assegura a

respectiva publicidade e presta outros serviços relativos a assinaturas digitais.

O certificado digital é o documento electrónico acessível em ambiente informático a qualquer interessado na sua consulta, que cria a certeza de que a pessoa que apõe uma assinatura digital é a titular da respectiva chave pública e, por conseguinte, também da respectiva chave privada.

Note-se que a verificação positiva de uma assinatura digital aposta num documento electrónico permite presumir que:

- a aposição da assinatura foi feita pelo respectivo titular ou seu representante, ou seja, desempenha uma função identificadora;

- aposição da assinatura foi feita com a intenção de subscrever o documento, ou seja, desempenha igualmente uma função finalizadora ou confirmadora; e
- o documento não sofreu nenhuma alteração posterior, ou seja, tem também uma função de inalterabilidade.

Quando os documentos electrónicos permitem que se façam as presunções acima elencadas e são susceptíveis de apresentação como declaração escrita, o legislador conclui que *são equiparados a documentos escritos particulares*, desempenhando, quando assinados, a função constitutiva do documento particular legalmente exigido como forma de negócio jurídico.

Em conclusão, quando lhe seja aposta uma assinatura electrónica qualificada certificada por uma entidade certificadora credenciada, o documento electrónico susceptível de apresentação como declaração escrita «tem a *força probatória de documento particular assinado, nos termos do 376.º do Código Civil*» (artigo 3.º, De-

creto-Lei n.º 290-D/99, de 2 de Agosto, sublinhado nosso). Ou seja, faz prova plena quanto às declarações atribuídas ao seu autor, sem prejuízo da arguição e prova da falsidade do documento. Porém, os factos só se consideram provados na medida em que forem contrários aos interesses do declarante.

No que concerne ao valor probatório dos documentos electrónicos que não revistam a forma escrita, atenda-se a que, se não tiverem a susceptibilidade de representação como declaração escrita mas tiverem aposta assinatura electrónica qualificada certificada, se submetem ao regime do artigo 368.º do Código Civil e do artigo 167.º do Código de Processo Penal. Ou seja, fazem prova plena dos factos e das coisas que representam, se a parte contra quem os documentos são apresentados não impugnar a sua exactidão.

Isto não obstante a utilização de outro meio de comprovação da autoria e integridade do documento electrónico, incluindo outras modalidades de assinatura electrónica, «desde que tal meio seja adoptado pelas partes ao abrigo de válida convenção sobre a prova ou seja aceite pela pessoa a quem for oposto o documento» (artigo 3.º, n.º 4). Sem prejuízo do exposto, os documentos sem assinatura electrónica qualificada certificada por entidade certificadora credenciada são apreciados livremente.

TESTE OS SEUS CONHECIMENTOS

1. Que modalidades de assinaturas electrónicas estabelece o Decreto-Lei n.º 62/2003, de 3 de Abril?
2. Quando é que o documento electrónico satisfaz o requisito legal de forma escrita? E quando é que vale como documento particular assinado?
3. Que requisitos preenche a assinatura electrónica avançada?

BIBLIOGRAFIA

- AAVV (1999), *Direito da Sociedade da Informação*, Coimbra, Coimbra Editora (Faculdade de Direito da Universidade de Lisboa e Associação Portuguesa do Direito Intelectual).
- BOCHURBERY, Lionel (1999), *Internet et Commerce Electronique*, 1.^a ed., Encyclopédie Delmas.
- GOMES VARGES, Mário (2006), *O Código da Privacidade e da Protecção de Dados na Lei e na Jurisprudência*, Famalicão, Centro Atlântico.
- GUERRA, Amadeu (1998), *Informática e Privacidade*, Lisboa, Vislis.
- GUERRA, Amadeu (2004), *A Privacidade no Local de Trabalho*, Coimbra, Almedina.
- LOPES ROCHA, MANUEL *et al.* (2001), *Leis do Comércio Electrónico, Notas e Comentários*, Coimbra, Coimbra Editora.
- LOPES ROCHA, MANUEL *et al.*, (2004), *Guia da Lei do Comércio Electrónico*, Famalicão, Centro Atlântico.
- LOPES ROCHA, Manuel, PUPO CORREIA, Miguel, FELINO RODRIGUES, Marta, ALMEIDA ANDRADE, Miguel e JOSÉ CARREIRO, Henrique (2001), *Leis do Comércio Electrónico – Notas e Comentários*, Coimbra, Coimbra Editora.
- MARQUES, Margarida, ANJOS, Mafalda e QUEIRÓZ VAZ, Sónia (2002), *101 Perguntas e Respostas do Direito da Internet e da Informática*, Vila Nova de Famalicão, Centro Atlântico.
- SARMENTO E CASTRO, Catarina (2005), *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina.



CAPÍTULO 1

A LEI DO COMÉRCIO ELECTRÓNICO 5

OBJECTO E ÂMBITO DE APLICAÇÃO 6

PRESTADORES DE SERVIÇOS DA SOCIEDADE DA INFORMAÇÃO 7

NOÇÃO 7

PRINCÍPIO DA LIBERDADE DE EXERCÍCIO .. 9

RESPONSABILIDADE DOS PRESTADORES DE SERVIÇOS EM REDE 11

ÂMBITO DE APLICAÇÃO 11

PRINCÍPIO DA EQUIPARAÇÃO 12

RESPONSABILIDADE POR SERVIÇOS DE SIMPLES TRANSPORTE 14

RESPONSABILIDADE POR SERVIÇOS DE ARMAZENAGEM INTERMEDIÁRIA 15

RESPONSABILIDADE POR SERVIÇOS DE ARMAZENAGEM PRINCIPAL 16

RESPONSABILIDADE POR SERVIÇOS DE ASSOCIAÇÃO DE CONTEÚDOS 18

AUSÊNCIA DE UM DEVER GERAL DE VIGILÂNCIA DOS PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS 19

DEVERES COMUNS DOS PRESTADORES INTERMEDIÁRIOS DE SERVIÇOS 19

SOLUÇÃO PROVISÓRIA DE LITÍGIOS 20

COMUNICAÇÕES PUBLICITÁRIAS EM REDE E *MARKETING* DIRECTO 22

ÂMBITO 22

IDENTIFICAÇÃO E INFORMAÇÃO 24

COMUNICAÇÕES NÃO SOLICITADAS 24

PROFISSÕES REGULAMENTADAS 25

CONTRATAÇÃO ELECTRÓNICA 25

ÂMBITO 25

PRINCÍPIO DA LIBERDADE

DE CELEBRAÇÃO 26

INFORMAÇÕES PRÉVIAS 27

PROPOSTA CONTRATUAL, ORDEM DE ENCOMENDA E AVISO DE RECEPÇÃO .. 28

CONTRATAÇÃO

SEM INTERVENÇÃO HUMANA 29

CAPÍTULO 2

A FACTURA ELECTRÓNICA 31

A LEI DA FACTURA ELECTRÓNICA 32

REQUISITOS LEGAIS 35

«AUTOFACTURAÇÃO» E EMISSÃO DE FACTURAS POR TERCEIROS 37

UTILIZAÇÃO DO EDI 38

UTILIZAÇÃO DA «ASSINATURA ELECTRÓNICA AVANÇADA» 40

A ASSOCIAÇÃO ALIANÇA DIGITAL 41

CAPÍTULO 3

PROTECÇÃO DE DADOS PESSOAIS 43

QUADRO DA LEGISLAÇÃO FUNDAMENTAL 44

A CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA 44

ALGUMAS DISPOSIÇÕES INTERNACIONAIS E EUROPEIAS 46

AS DISPOSIÇÕES JURÍDICAS NACIONAIS .. 52

ALGUMAS NOÇÕES ESSENCIAIS 56

DADOS PESSOAIS 57

TRATAMENTO DE DADOS PESSOAIS 58

O TRATAMENTO DE DADOS PESSOAIS: CONDIÇÕES DE LEGITIMIDADE 59

A OBRIGAÇÃO DE NOTIFICAÇÃO DO TRATAMENTO, AS ISENÇÕES DE NOTIFICAÇÃO E O CONTROLO PRÉVIO DA CNPD (AUTORIZAÇÃO) 59

A obrigação de notificação do tratamento 59

As isenções de notificação 60

O controlo prévio da CNPD (a autorização) 61

OS FUNDAMENTOS DO TRATAMENTO 62

OS DADOS PESSOAIS SENSÍVEIS	63	PRINCÍPIOS SUBJACENTES	
OS DIREITOS DOS TITULARES		AO TRATAMENTO DE DADOS	
DOS DADOS	64	PESSOAIS	66
A TRANSFERÊNCIA INTERNACIONAL		A TUTELA DOS DADOS PESSOAIS	67
DE DADOS PESSOAIS	64		
TRANSFERÊNCIAS DENTRO DA UNIÃO		CAPÍTULO 4	
EUROPEIA	64	A ASSINATURA ELECTRÓNICA	69
TRANSFERÊNCIAS PARA UM ESTADO		ENQUADRAMENTO LEGISLATIVO	70
QUE NÃO PERTENÇA À UNIÃO		A NOÇÃO LEGAL DE DOCUMENTO	
EUROPEIA	65	ELECTRÓNICO	71
TRANSFERÊNCIAS PARA UM ESTADO		VALOR PROBATÓRIO	71
QUE NÃO ASSEGURE UM NÍVEL DE		A CERTIFICAÇÃO DA ASSINATURA	73
PROTECÇÃO ADEQUADO	65		
TRANSFERÊNCIAS REALIZADAS		REFERÊNCIAS	77
AO ABRIGO DE CLÁUSULAS			
CONTRATUAIS-TIPO APROVADAS			
PELA COMISSÃO EUROPEIA	66		
SEGURANÇA E CONFIDENCIALIDADE			
DO TRATAMENTO DE DADOS PESSOAIS ...	66		