1. A proteção de dados pessoais do trabalhador no âmbito da relação de trabalho

Worker's data protection in an employment relationship

(Autor)

TIAGO PIMENTA FERNANDES

Professor Adjunto Convidado do Instituto Politécnico do Porto; Professor Auxiliar da Universidade Portucalense; IJP - Instituto Jurídico Portucalense; Advogado tvmf@iscap.ipp.pt; tiagof@upt.pt

Sumário:

Área do Direito: Trabalho

Resumo:

A recente aprovação, pela União Europeia, do Regulamento Geral de Proteção de Dados (RGPD) veio revolucionar o enquadramento jurídico que permite que as empresas procedam ao tratamento de dados pessoais a que estas tenham acesso, designadamente, no âmbito de uma relação de trabalho. Efetivamente, são inúmeras as situações em que, no dia-a-dia empresarial, uma empresa recebe, acede, trata, transmite e, por vezes até, expõe os dados pessoais daqueles que para si trabalham. Perante isto, impõe-se o estudo atento desta nova normativa que invadiu o ordenamento jurídico dos Estados-Membros.

Abstract:

The recent adoption by the European Union of the General Data Protection Regulation (GPDR) has revolutionized the legal frame which allows companies to handle personal data to which they

have access, particularly, within an employment relationship. In fact, there are innumerable situations in which a company receives, accesses, handles, transmits or even exposes the personal data of their employees. Therefore, it is necessary to carefully study this new legislation which has invaded the legal order of the Member States.

Palavras-Chave: proteção, dados, pessoais, regulamento, trabalhador
Keywords: protection, data, personal, regulation, labour, worker

1. Enquadramento jurídico

[1]Historicamente, as primeiras preocupações legislativas com a questão da proteção dados fizeram-se sentir nos normativos sobre Direitos Humanos, com a Declaração Universal dos Direitos do Homem[2] a prever, pela primeira vez, normas específicas relacionadas com o direito à privacidade e vida familiar (artigo 12º), que estiveram na antecâmara das normas europeias sobre proteção de dados e privacidade. Por seu turno, a Convenção Europeia dos Direitos do Homem ressaltou a proteção da vida privada (artigo 8º), entre outros direitos.

Entre o final dos anos sessenta e os anos oitenta, diversos países europeus adotaram, pela primeira vez, legislação destinada a controlar o uso de informação privada por parte de empresas e governos. Em Portugal, tal como em outros países (Espanha e Áustria, p. ex.) a proteção de dados passou a constar da lei fundamental, assumindo dignidade Constitucional (art. 35.º). Já em 2000, a Carta dos Direitos Fundamentais da União Europeia[3], que veio consolidar a temática dos direitos fundamentais dentro da União, previa no seu artigo 8.º o "direito à proteção de dados de carácter pessoal, o tratamento leal e para fins específicos, o direito de acesso e retificação", sob a epígrafe "proteção de dados pessoais".

Nos últimos cinco anos, a União Europeia tem-se revelado particularmente atenta às questões da proteção de dados, para o que contribuiu certamente a verificação de um maior volume de dados que atualmente circulam na rede, a crescente colaboração entre participantes da Internet, o surgimento de empresas diferentes no mercado, a maior complexidade dos sistemas integrados na internet (*cloud*, *computing*, *big data*), a multiplicação de dados gerados (nome, morada, dados de localização, IP's), entre outros fatores.

Nesse seguimento, surgiu recentemente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (diploma a que doravante nos referiremos através da sigla RGPD), que revogou a Diretiva 95/46/CE, que até então regulava a matéria da proteção de dados no âmbito europeu[4].

Na sua essência, o RGPD veio harmonizar a legislação sobre proteção e tratamento de dados pessoais, tornando clara e transversal a política a seguir por todos os que recolhem e tratem dados pessoais, do mesmo modo que protege e fortalece a privacidade de dados pessoais dos residentes da União Europeia, devolvendo-lhes o controlo sobre os mesmos, e remodelou a forma como as organizações deverão abordar a privacidade dos dados pessoais daqueles com quem lidam, nomeadamente, dos seus trabalhadores.

O referido Regulamento, dada a sua natureza jurídica, não carece de transposição, sendo imediatamente aplicável a todos os Estados-Membros, superiorizando-se mesmo a quaisquer normas internas que disponham em sentido diverso, por força do princípio do primado do direito comunitário. De acordo com o referido princípio, aplicável a todos os atos europeus com força vinculativa, o direito europeu tem um valor superior ao dos direitos nacionais dos Estados-Membros, o que impede os Estados-Membros de aplicarem uma regra nacional contrária ao direito europeu[5].

2. A "nova" proteção de dados pessoais do trabalhador

2.1. Âmbito de aplicação do diploma

Do ponto de vista material, o RGPD reputa-se aplicável ao tratamento de dados pessoais, automatizado ou não automatizado (art. 2.º, n.º 1), entendendo-se por dado pessoal toda a informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"). O Regulamento esclarece que será considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (art. 4.º, n.º 1). Por seu turno, o conceito de tratamento, igualmente relevante, é definido de modo abrangente, como uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (art. 4.º, n.º 2).

No contexto laboral, são várias as situações que, de imediato, este conceito nos suscita e que poderão implicar o tratamento de dados pessoais do trabalhador. Pense-se, p. ex., na mera referência a um trabalhador numa página da internet da empresa e a sua identificação pelo nome ou telefone, no processamento de salários, na elaboração de procedimentos disciplinares, na comunicação com entidades terceiras (como a Segurança Social e a ACT, por exemplo), no preenchimento de relatório único, no recrutamento, entre outras.

Ao nível dos sujeitos abrangidos pelo RGPD, alude-se a uma atividade exercida em contexto de um estabelecimento de um responsável pelo tratamento ou de um subcontratante" (art. 3.º, n.º 1), entendendo-se por "responsável de tratamento" toda a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais (art. 4.º, n.º 7) e por subcontratante a "pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (n.º 8), como será o caso, p. ex., de uma empresa que se ocupe apenas da área de recursos humanos de uma outra, empregadora.

Ao nível do titular dos dados, parece claro que o RGPD se aplica à figura do trabalhador, desde o momento do acesso ao emprego à cessação do contrato de trabalho, e independentemente da natureza do seu vínculo jurídico (abrangendo o mero prestador de serviços, o trabalhador temporário ou mesmo o estagiário).

Do ponto de vista territorial, o Regulamento incide sobre as situações em que o tratamento de dados pessoais seja efetuado situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, pese embora em alguns casos estenda a sua aplicabilidade a situações em que o responsável de tratamento ou subcontratante não se encontrem naquele território (art. 4.º, n.os 1 e 2).

2.2. Princípios gerais

São vários os princípios que enformam o RGPD em matéria de tratamento de dados pessoais, e dos quais retiramos importantes consequências práticas para quem venha a ser envolvido por esse tratamento.

Em primeiro lugar, assinalamos o *princípio da licitude* (art. 6.º), segundo o qual o tratamento de dados pessoais será lícito quando se verifique uma das seguintes situações: a) a existência de consentimento por parte do titular dos dados; b) a execução de um contrato ou diligências pré-contratuais a pedido do titular dos dados; c) cumprimento de obrigação legal[6]; d) defesa dos interesses vitais do titular; e) o exercício de funções de interesse público ou por uma autoridade pública; e ainda a verificação de f) interesses legítimos do responsável pelo tratamento ou de terceiros.

Uma nota particular nos merece o consentimento, por se antever que esta venha a ser uma das

principais formas de contornar a ilicitude do tratamento de dados pessoais a que empregador venha a recorrer. Em primeiro lugar, o Regulamento exige que esse consentimento do titular dos dados seja concedido para uma finalidade que deverá estar claramente definida. Por outro lado, tal ato deverá ser livre, informado, e exprimir-se por um ato inequívoco do titular dos dados. Daí que o consentimento deva ser dado de forma positiva (por escrito ou por meio eletrónico, ou mesmo verbalmente), e nunca extrair-se de uma inação do trabalhador (p. ex., como resultado de um silêncio do trabalhador, ou de *pre-ticked boxes* criadas para o efeito). Quanto à "liberdade" de tal consentimento, a mesma sempre será de questionar no âmbito laboral, em que não vigora propriamente uma igualdade de armas, sobretudo em situações especialmente delicadas para o trabalhador (pense-se, p. ex., no momento do recrutamento, ou em que o pedido de consentimento é feito no âmbito de uma avaliação de desempenho do trabalhador). De resto, o RGPD é claro ao estipular que, se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples (art. 7.º, n. 2) e que o trabalhador deverá ter sempre o direito revogar o consentimento (n.º 3).

Prevê-se agora um regime distinto para o tratamento de categorias especiais de dados pessoais, quando estejam em causa dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (art. 9.º, n.º 1). Em tais casos, o tratamento será proibido, com exceção das situações elencadas no n.º 2 da referida norma. Destacamos nesta sede a filiação sindical e os dados biométricos como dados cujo tratamento poderá muitas vezes estar em causa no âmbito de uma relação laboral

De acordo com o *princípio da transparência* (art. 12.º), o responsável pelo tratamento fica obrigados a informar o trabalhador e a mantê-lo informado sobre o modo como os seus dados estão a ser utilizados. Deverá ainda documentar o modo como se propõe tratar os respetivos dados. O responsável pelo tratamento tomará as medidas adequadas para fornecer ao titular as informações devidas (arts. 13.º e 14.º) e qualquer comunicação (arts. 15.º a 22.º e 34.º) a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. As informações serão prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos[7]. Tal informação deverá ser prestada sem demora injustificada, e no prazo de um mês a contar da data de receção do pedido, o qual admite prorrogação até dois meses, quando necessário, tendo em conta a complexidade do pedido e o número de pedidos apresentados (art. 12.º, n.º 3). Prevê-se, assim, um novo dever de informação, que ficará a cargo do empregador (quando seja este o responsável pelo tratamento dos dados), e que acrescerá aos que sobre si já impendem[8].

De acordo com o *princípio da especificação e da limitação da finalidade*, a legitimidade do tratamento de dados pessoais dependerá da finalidade do tratamento, a qual terá de ser especificada e comunicada antes do início do tratamento dados pessoais. Significa isto que, sempre que os dados forem tratados para uma nova finalidade, será preciso um novo fundamento legal que o legitime, e assim sucessivamente[9].

De acordo com o *princípio da minimização e exatidão dos dados*, os dados pessoais devem ser adequados, pertinentes e não excessivos relativamente à finalidade para que são recolhidos e para que são tratados posteriormente. Já segundo o *princípio da limitação da conservação dos dados*, os mesmos deverão ser conservados de forma a permitir a identificação das pessoas apenas durante o período de tempo necessário para a prossecução das finalidades para as quais forma recolhidos ou para que são tratados posteriormente, abstendo-se o RGPD de prever qual a extensão concreta deste período. Na verdade, entrega-se ao responsável pelo tratamento (ou, se for o caso, ao subcontratante) a definição do período temporal dentro do qual este poderá ficar na posse de tais dados, cabendo-lhe ainda a importante tarefa de se certificar acerca dos motivos que, em cada caso, justificarão a necessidade dessa conservação. Aceita-se, no entanto, que por vezes essa necessidade possa decorrer de soluções legais que tornam razoável a conservação de tais dados. A título de exemplo, aceita-se que o prazo de prescrição que atribui ao trabalhador (bem como ao

empregador) a possibilidade de reclamar créditos emergentes de contrato de trabalho, da sua violação ou cessação, dentro de um ano a partir do dia seguinte àquele em que cessou o contrato de trabalho[10], funcionará como um índice temporal mínimo para a conservação de tais dados após a cessação do vínculo laboral.

Alude-se ainda a um *princípio da integridade* e de *confidencialidade* dos dados, nos termos dos quais os dados pessoais sob tratamento deverão ser seguros e confidenciais, o que exigirá de que procede ao seu tratamento a disponibilidade de equipamento adequado para o efeito, alertando-se para a importância de os trabalhadores serem devidamente informados relativamente às regras de segurança no tratamento de dados.

Por fim, de acordo com o *princípio da responsabilidade*, exige-se do responsável pelo tratamento dos dados que este aplique as medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com o Regulamento (art. 24.º), nomeadamente, através do cumprimento de códigos de conduta (art. 40.º) ou de procedimentos de certificação aprovados (art. 42.º), sob pena de responsabilização pelos danos (materiais e imateriais) que o incumprimento do RGPD possa originar (art. 82.º, n.º 1).

2.3.A atribuição de novos direitos

Por via do RGPD, o titular dos dados vê serem-lhe atribuídos novos direitos nesta matéria.

Em primeiro lugar, um *direito ao esquecimento*: o Regulamento é claro ao prever que o titular tem direito a solicitar a eliminação dos dados, a qualquer momento, quando se verifique algum dos motivos previstos no n.º 1 do art. 17.º. Em segundo lugar, um *direito de portabilidade*, nos termos do qual o titular tem, em certas ocasiões o direito de transmitir os seus dados pessoais a outro responsável pelo tratamento, sem poder ser impedido (art. 20.º). O art. 15.º atribui ao titular um *direito ao acesso à informação*, que se traduz na possibilidade de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais. Por último, um *direito de oposição*, que possibilita que o titular dos dados se oponha ao tratamento dos dados pessoais que lhe digam respeito, incluindo a definição de perfis com base nessas disposições, por motivos relacionados com a sua situação particular (art. 21.º).

3.O Subcontratante e o Encarregado de Proteção de Dados (DPO)

O Regulamento prevê expressamente a possibilidade de o tratamento dos dados ser efetuado por um subcontratante, caso em que o responsável pelo tratamento deverá ter o cuidado de recorrer apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas (art. 28.º, n.º 1). Por seu turno, o subcontratante não poderá contratar outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações (n.º 2).

O tratamento em subcontratação é regulado por contrato ou outro ato normativo, estabelecendo o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento (n.º 3).

De salientar que, nos termos do Regulamento, o subcontratante terá obrigações e responsabilidades diretas, pelo que responderá pelos danos causados pelo tratamento caso não tenha cumprido as obrigações decorrentes do RGPD dirigidas especificamente aos subcontratantes, ou não tenha seguido as instruções lícitas do responsável pelo tratamento (art. 82.º, n.º 1 e 2).

Um ponto em que o RGPD inova consiste na criação e regulamentação da figura do Encarregado de Proteção de Dados (*Data Protection Officer – DPO*), a quem caberá essencialmente assessorar o

responsável pelo tratamento, subcontratante e/ou trabalhadores, com vista ao pleno cumprimento da lei em matéria de proteção de dados, verificar a conformidade das políticas do responsável ou do subcontratante relativas à proteção de dados pessoais; emitir parecer no âmbito das avaliações de impacto, bem como controlar a realização dessas avaliações, e ainda cooperar e interagir com a autoridade de supervisão (39.º).

A nomeação de encarregado de proteção de dados será obrigatória sempre que o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais, as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala, ou quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais sensíveis ou relacionados com condenações penais e infrações (37.º, n.º 1).

O DPO deverá ser designado com base nas suas qualidades profissionais e conhecimentos especializados na área da proteção de dados, devendo ser envolvido em todas as questões relacionadas com a proteção de dados pessoais. Funcionará como uma ponte entre o responsável pelo tratamento de dados e o titular, admitindo-se a possibilidade de ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços (art. 37.º, n.º 6).

4. Conclusões

De um modo sintético, pode dizer-se que o RGPD veio estabelecer alterações significativas no contexto da proteção e segurança do tratamento de dados pessoais dentro da União, passando de um modelo marcadamente heterorregulador para um modelo autorregulador da empresa, em que passa a ser esta a ter de implementar mecanismos internos para assegurar o cumprimento das normas reguladoras nesta matéria. À primeira vista, a implementação do Regulamento significará para muitas empresas uma mudança organizacional muito significativa, com implicações operacionais evidentes, que obrigará os agentes a avaliar e rever todos os processos por si até então implementados na empresa nesta matéria, dado que o mesmo se reputa aplicável a todos os dados detidos e/ou tratados pela empresa à data da entrada em vigor do diploma. A consciencialização dos agentes para a importância da identificação e avaliação dos riscos de privacidade parece-nos, assim, inevitável, e assume-se como um objetivo claro do Regulamento.

Nessa linha, sugere-se a adoção de várias medidas pelos empregadores, nomeadamente, a adoção de um regulamento interno ou código de conduta sobre estas matérias, a criação de uma política de proteção de dados, não só em matéria de interação com os trabalhadores da empresa, mas também na relação entre esta e outros entes externos (fornecedores, parceiros, etc.). Em obediência à filosofia de autorregulação proclamada, será também de esperar que o empregador implemente mecanismos de consentimento válidos e sistemas de monitorização e controlos adequados, bem como um sistema eficaz de gestão de riscos de privacidade, que tenha em funções um encarregado de proteção de dados, zelando sempre pelo respeito dos direitos dos titulares dos dados pessoais em causa, e mantendo sempre um fiel e evidente registo de que o Regulamento é cumprido em toda a linha.

Por outro lado, um *compliance* contínuo da empresa nesta matéria, nomeadamente, ao nível da avaliação do impacto aquando da introdução quando um novo tipo de tratamento de dados é introduzido (*privacy impact assessment*), bem como da identificação regular e atenta das vulnerabilidades de intrusão e acesso aos dados (*vulnerability mapping e intrusion test*), que permitam aferir os mecanismos de prevenção necessário, afigura-se-nos igualmente fulcral.

Em cada Estado-Membro será de esperar a criação de normas internas que permitam clarificar alguns aspetos sobre esta matéria, nos termos do art. 88.º do RGPD, que prevê que

> "Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de

dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho (...), bem como para efeitos de cessação da relação de trabalho".

Salienta-se, no entanto, que a margem de implementação que é dada aos Estados-Membros se afigura extremamente reduzida. Em Portugal, encontra-se sob estudo e preparação uma proposta de Regulamento Nacional sobre esta matéria, sendo o respetivo conteúdo por nós desconhecido à data da submissão do presente artigo.

NOTAS AL PIE DE PÁGINA

1

Este trabalho foi elaborado no âmbito do projeto de investigação MINECO (DER2016-75376-R) coordenado pela Professora Lourdes Mella Méndez.

2

Aprovada pela assembleia geral da ONU em 10 de dezembro 1948.

3

2000/C 364/01.

4

Numa perspetiva de enquadramento geral da matéria em sede de direito europeu, salientam-se outros diplomas igualmente relevantes sobre esta matéria: Diretiva 2002/58 / CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (alterada pela Diretiva 2009/136/CE) [a Diretiva e-Privacy]; o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e órgãos comunitários e à livre circulação desses dados; Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, revogada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para fins de prevenção, investigação, deteção ou repressão de crimes, infrações ou execução de sanções penais e sobre a livre circulação desses dados [Diretiva relativa aos Dados Criminais]; Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão [Regulamento Transparência e Acesso aos Documentos]. Ao nível do Conselho da Europa, salientam-se a Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais (CEDH), bem como a Convenção para a proteção dos indivíduos relativamente ao tratamento automatizado de dados de carácter pessoal, ETS N.º. 108, 28.1.1981 (Convenção n.º 108). No plano das decisões da Comissão Europeia sobre a transferência de dados, assumem especial relevância as seguintes: Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de

dezembro de 2016, que altera as Decisões 2001/497/CE e 2010/87/UE relativas às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros e para subcontratantes estabelecidos nesses países, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho; Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho; 2010/87/CE: Decisão da Comissão, de 5 de Fevereiro de 2010 , relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho; 2004/915/CE: Decisão da Comissão, de 27 de Dezembro de 2004, que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros.

5

Trata-se de um princípio fundamental do direito europeu. Tal como o princípio do efeito direto, não está consignado nos Tratados, tendo sim sido consagrado pelo Tribunal de Justiça da União Europeia (TJUE) no acórdão Costa contra Enel de 15 de julho de 1964. Neste acórdão, o Tribunal declara que o direito proveniente das instituições europeias se integra nos sistemas jurídicos dos Estados-Membros, sendo estes obrigados a respeitá-lo. O direito europeu tem assim o primado sobre os direitos nacionais. Deste modo, se uma regra nacional for contrária a uma disposição europeia, as autoridades dos Estados-Membros devem aplicar a disposição europeia.

6

A título de exemplo, inserem-se aqui as várias comunicações encetadas pelo empregador junto da Segurança Social e que implicam o tratamento de dados dos trabalhadores envolvidos.

7

Prevê-se a possibilidade de a informação ser prestada oralmente, caso o titular dos dados o solicitar, desde que a identidade deste seja comprovada por outros meios.

8

No direito português, os deveres de informação do empregador encontram-se previstos no n.º 3 do art. 106.º do Código do Trabalho.

9

A título de exemplo, a recolha de dados dos trabalhadores para registo de horas trabalhadas não poderá ser usada para o preenchimento do Relatório Único da empresa.

10

Nos termos do n.º 1 do no art. 337.º do Código do Trabalho português.