DIREITO DA PROTECÇÃO DE DADOS PESSOAIS

ALGUMAS NOTAS SOBRE O REGULAMENTO GERAL DE PROTECÇÃO DE DADOS

Apesar de ter entrado em vigor a 25 de Maio de 2016, 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 e que revoga a Diretiva 95/46/CE (RGPD), é aplicável desde 25 de Maio de 2018.

O RGPD vem introduzir uma profunda mudança de paradigma a nível da União Europeia na forma de tratar os dados pessoais, merecendo, por esse motivo, uma análise aos seus principais aspectos.

I – Âmbito de Aplicação

O RGPD 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 ou a eles destinados.

Os dados pessoais correspondem a qualquer informação, relativamente a uma pessoa singular identificada ou identificável, de qualquer natureza e independentemente do tipo de suporte, como, por exemplo, o nome, o endereço de e-mail ou o número de contacto telefónico.

A noção de tratamento de dados, por sua vez, inclui a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Estão excluídos do âmbito de aplicação do RGPD o tratamento de dados efectuados no exercício de actividades não sujeitas à aplicação do Direito da União. Também não se aplica às questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com actividades que se encontrem fora do âmbito de aplicação do Direito da União, bem como as que se prendem com a segurança nacional. O tratamento de dados pessoais pelos Estados-Membros no exercício de actividades relacionadas com a política externa e de segurança comum da União, bem como o tratamento de dados pessoais efectuado por pessoas singulares no exercício de actividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma actividade profissional ou comercial ficam igualmente afastados do âmbito de aplicação. Por último, o RGPD não se aplica ao tratamento de dados efectuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Quanto ao âmbito de aplicação territorial, o RGPD aplica-se ao tratamento de dados pessoais efectuado no contexto das actividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

Também se aplica ao tratamento de dados pessoais das pessoas que **se encontram** no território da União, efectuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as actividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento, bem como as relacionadas com o controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

Desta forma, louvamos a rectificação publicada no JOUE, no dia 23 de Maio de 2018, que corrigiu a tradução portuguesa do artigo 3.º do RGPD, quando referia a aplicação ao tratamento de dados pessoais **de residentes** da União Europeia. A versão inglesa, que foi a versão de trabalho, é muito clara ao estipular que *"This Regulation applies to the processing of personal data of **data subjects who are in the Union**"*, não fazendo, desta forma, qualquer referência ao critério da residência. Também o Considerando n.º 14 não deixa dúvidas quando dispõe que *"a proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da*

sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais".

É, assim, pacífico que o RGPD se aplica, em regra, ao tratamento de dados pessoais que são realizados no espaço da União Europeia, independentemente de o titular dos direitos ser ou não residente num país da União.

II – Princípios Relativos à Protecção de Dados

O tratamento dos dados, de acordo com o RGPD, apenas poderá ser efectuado respeitando princípios basilares, de forma a proteger o titular desses direitos.

Os **princípios da licitude, da lealdade e da transparência** pressupõem que os dados pessoais apenas poderão ser tratados se for lícito o seu tratamento, nos casos previstos no artigo 6.º do RGPD, e desde que seja observado um comportamento leal e transparente relativamente ao titular dos dados.

O princípio da limitação das finalidades exige que os dados recolhidos para uma finalidade apenas possam ser tratados para essa finalidade, exceptuando o tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica, bem como para fins estatísticos.

A apreciação pelo responsável pelo tratamento da compatibilidade do tratamento com outras finalidades diferentes das que justificaram a respectiva recolha está sujeita aos requisitos apertados do n.º 4 do art. 6.º.

O princípio da minimização de dados dispõe que os dados pessoais a recolher devem ser adequados, pertinentes e limitados ao estritamente necessário para prossecução da finalidade para o qual é tratado.

O princípio da exactidão prevê que os dados devem ser exactos e actualizados sempre que necessário, devendo os dados inexactos ser apagados ou rectificados sem demora.

O princípio da limitação da conservação impõe o dever de conservação dos dados de uma forma que permita a identificação dos titulares dos dados apenas pelo período necessário para as finalidades pelo qual estes são tratados.

O princípio da integridade e confidencialidade exige que os dados sejam tratados de uma forma que garanta a sua segurança, incluindo a protecção contra o seu

tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adoptando as medidas técnicas ou organizativas adequadas.

O princípio da responsabilidade estabelece que o responsável pelo tratamento é o responsável pelo cumprimento das regras de tratamento de dados, tendo o ónus de o comprovar.

Apesar de não constar do elenco do RGPD, o **princípio da proporcionalidade** é transversal a toda a actividade de tratamento de dados, devendo ser uma bússola que norteia toda a actividade quer do responsável pelo tratamento e do subcontratante, quer da autoridade de controlo.

III – A licitude do tratamento

Como referido, um dos princípios basilares da proteção de dados é a obrigatoriedade de licitude do tratamento dos dados.

O RGPD dispõe, no seu artigo 6.º, que o tratamento apenas se considera lícito se e na medida em que se verifiquem certas situações que tipifica.

Um dos fundamentes de licitude do tratamento de dados é através do **consentimento do titular** para uma ou mais finalidades específicas. Quando o tratamento for realizado com base neste consentimento, o responsável pelo tratamento deve demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

Se o consentimento for prestado no contexto de uma declaração escrita, o que é aconselhável, pois esta consubstancia uma evidência do consentimento para o tratamento de dados, o pedido deverá ser apresentado numa linguagem clara e simples. A todo o momento, o titular dos dados pode retirar o consentimento, devendo ser informado dessa faculdade, antes de prestar o consentimento. É importante salientar que o RGPD exige que o consentimento deve ser tão fácil de retirar quanto de dar, sendo certo que a conclusão do contrato não pode estar subordinada ao mesmo, quando o tratamento de dados pessoais não seja necessário para a respectiva execução.

Relativamente aos menores, em concreto quanto à oferta directa de serviços da sociedade de informação, o consentimento apenas é lícito se eles tiverem, pelo menos, 16 anos, podendo os Estados-Membros dispor de uma idade inferior, desde que essa idade não seja inferior a 13 anos.

Parece que o legislador nacional aproveitará essa excepção, visto que a Proposta de Lei n.º 120/XIII, que não foi aprovada no dia 4 de Maio de 2018, tendo entretanto baixado novamente à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, pelo período de 45 dias, prevê, no seu artigo 16.º, n.º 1, a idade mínima de 13 anos para a licitude do consentimento de menores nestas situações, apesar do parecer contrário da CNPD, que aconselha, com pertinência, o critério fixado no Código Penal, no artigo 38.º, n.º 3, de 16 anos.

O tratamento de dados é também tido por lícito se for necessário para a **execução de um contrato** no qual o titular dos dados é parte ou para diligências pré-contratuais a pedido do titular dos dados.

Se o tratamento for necessário para o **cumprimento de uma obrigação legal,** expressão preferível à também pouco precisa obrigação jurídica, a que o responsável pelo tratamento esteja sujeito, considera-se lícito esse tratamento. A obrigação legal deverá assentar no Direito da União ou do Estado-Membro, devendo cabendo a cada um destes ordenamentos jurídicos definir qual a finalidade do tratamento dos dados.

Estando em causa **a defesa de interesses vitais do titular dos dados ou de outra pessoa singular**, o tratamento igualmente se tem por lícito. No entanto, este tratamento só pode ter lugar quando o tratamento não se puder basear noutro fundamento jurídico. Um exemplo de tipo de tratamento para defesa de interesses vitais do titular dos dados, que também serve um importante interesse público, é o caso do tratamento para fins humanitários, incluindo a monitorização de epidemias e da sua propagação, bem como situações de emergência humanitária, em especial, em situações de catástrofes naturais e de origem humana.

Também é lícito o tratamento necessário ao **exercício de funções de interesse público** ou ao **exercício da autoridade pública** de que está investido o responsável pelo tratamento. Porém, o tratamento deverá sempre obedecer aos princípios basilares previstos no RGPD, nomeadamente, o princípio da limitação da finalidade. Além disso, a entidade pública deve fazer o tratamento, de acordo com o princípio da especialidade dos fins, ou seja, apenas na prossecução dos fins que lhe foram atribuídos, e na sua justa medida.

É, igualmente, lícito o tratamento quando este for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, tendo em conta as expectativas razoáveis dos

titulares dos dados baseadas na relação com o responsável. Poderá, tal como refere o Considerando n.º 47, haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. Esse interesse legítimo será sempre objecto de uma avaliação casuística e cuidada, em contraponto com os direitos e liberdades pessoais do titular.

IV – Tratamento de categorias especiais de dados pessoais

O RGPD, no artigo 9.º, regula o tratamento de categorias de dados pessoais que se consideram especiais.

A regra, presente no n.º 1 desse artigo, é a de que *"é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"*.

O n.º 2 do artigo 9.º elenca várias excepções a esta proibição.

Assim, a prestação de consentimento explícito por parte do titular dos dados para o tratamento desses dados pessoais especiais para uma ou mais finalidades específicas constitui uma forma de licitude do tratamento destes dados, excepto se houver uma proibição expressa do Direito da União ou de um Estado-Membro.

No caso de o tratamento ser necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, se legalmente permitido, também será considerado lícito.

O tratamento necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento, também é considerado lícito.

Também estará excluído desta proibição o tratamento efectuado, no âmbito das suas actividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins

políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares.

É analogamente lícito o tratamento de dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular, bem como se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional.

No âmbito da medicina, sempre pressupondo a obrigação de sigilo por parte dos profissionais de saúde, o tratamento será lícito se for necessário para a medicina preventiva ou do trabalho, a avaliação da capacidade de trabalho do empregado, diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no Direito da União ou dos Estados-Membros ou se tiver como fundamento a execução de um contrato com um profissional de saúde.

Está também excluído da proibição do n.º 1, o tratamento de dados justificado por motivos de interesse público importante, com base no Direito da União ou de um Estado-Membro, devendo ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados. Em especial, no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no Direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

Por fim, será lícito o tratamento desses dados se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica, bem como fins estatísticos. Nestes casos, deverá ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados

V – Direitos dos titulares dos dados

Os titulares dos dados gozam de um conjunto de direitos que lhe são conferidos pelo RGPD.

Neste elenco, estão incluídos o direito a receber um conjunto de informações referentes à finalidade, prazo de conservação, categoria de dados e destinatários sempre que os dados pessoais não sejam recolhidos junto do titular, entre outras; o direito a aceder aos dados pessoais e a ser informado sobre a finalidade, a categoria de dados, os destinatários dos dados a quem os dados foram ou são divulgados, o prazo de conservação e o direito a apresentar reclamação a uma autoridade de controlo; o direito à rectificação dos seus dados em caso de incorrecção; o direito ao apagamento (direito a ser esquecido); o direito à limitação do tratamento de dados para qualquer outro fim que não o referido aquando da sua obtenção, recaindo sobre o responsável uma obrigação de notificação da rectificação ou apagamento dos dados pessoais ou limitação do tratamento; o direito à portabilidade dos dados, ou seja, a obrigação por parte da empresa de fornecer os dados na totalidade num formato digital de fácil acesso; o direito de se opor, a qualquer momento, ao tratamento dos dados pessoais que lhe digam respeito com base no exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros e quando, estando em causa o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do Direito da União ou dos Estados-Membros; e os direitos relacionados com o repúdio de decisões individuais automatizadas, incluindo definição de perfis, ou seja, o direito a exigir uma intervenção humana no processamento de dados.

VI – Responsável pelo tratamento e subcontratante

O responsável pelo tratamento, como define o RGPD, é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras entidades, determina as finalidades e os meios de tratamento de dados pessoais. Como é o responsável pelo tratamento que se encontra em poder dos dados pessoais, e foi este que definiu as finalidades e os meios de tratamento dos

mesmos, deve ser ele a aplicar as medidas técnicas e organizativas que forem adequadas para **assegurar e poder comprovar** que o tratamento é realizado em conformidade com o RGPD.

Assim, sempre que este utilize um subcontratante, que, em rigor, deveria ser designado de subcontratado, para tratar os dados, incumbe ao responsável pelo tratamento garantir que o subcontratante apresenta garantias suficientes de execução de medidas técnicas e organizativas adequadas a que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos do titular dos dados.

É ainda necessário que o tratamento no âmbito da subcontratação seja regulado por contrato ou por outro acto normativo ao abrigo do Direito da União Europeia, vinculando o subcontratante ao responsável pelo tratamento.

Esse contrato deve estabelecer o objecto e a duração do tratamento, a natureza e a finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados e ainda as obrigações e direitos do responsável pelo tratamento.

No que ao tratamento diz respeito, o responsável pelo tratamento e, se caso disso, o seu representante, devem conservar um registo de todas as actividades de tratamento sob sua responsabilidade.

Tal registo deverá conter não só o nome e o contacto do responsável pelo tratamento, como ainda as finalidades do tratamento, a descrição das categorias de titulares de dados e de dados pessoais, as categorias de destinatários a quem os dados pessoais foram ou serão divulgados, as transferências de dados que forem efectuadas para países terceiros ou organizações internacionais, os prazos, se for possível determiná-los, previstos para o apagamento das diferentes categorias de dados, bem como, se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

É importante sublinhar que, apesar de a obrigação de registo de tratamento de dados não se aplicar a empresas ou organizações com menos de 250 trabalhadores, é exigido o registo sempre que o tratamento efectuado seja susceptível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados ou dados pessoais relativos a condenações penais e infracções.

Sobre os responsáveis pelo tratamento e os subcontratantes recai um dever de cooperação com a autoridade de controlo, no âmbito do qual devem facultar-lhe os registos de tratamento de dados, sempre que tal for solicitado.

VII – Avaliação de impacto sobre a protecção de dados e consulta prévia

A obrigatoriedade de realizar uma avaliação de impacto pelo responsável pelo tratamento antes de proceder ao tratamento de certo tipo de dados é mais uma novidade que este RGPD nos traz.

De facto, tal obrigação tem por base a mudança de paradigma que agora se desenhou nas competências das autoridades de controlo, que deixou de realizar um controlo prévio sobre certos tratamentos de dados para, ao mesmo tempo que transfere a responsabilidade desse controlo prévio para o responsável pelo tratamento, assumir uma função meramente inspectiva de cumprimento das obrigações do responsável pelo tratamento.

Assim, sempre que um certo tipo de tratamento for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, em particular quando utilize novas tecnologias, existe a obrigação do responsável pelo tratamento, antes mesmo de o iniciar, realizar a avaliação de impacto das operações a concretizar sobre os dados pessoais.

Por mero exemplo, quando um responsável pelo tratamento desejar colocar câmaras de videovigilância, o que até agora exigia um parecer prévio positivo da CNPD e ainda exige no art. 21º do Código do Trabalho, em face do novo RGPD fica apenas dependente da avaliação de impacto desse tratamento de dados sobre os dados pessoais pelo responsável pelo tratamento.

Apenas haverá a consulta prévia da autoridade de controlo no caso de ser realizada a avaliação de impacto e se concluir que o tratamento resultaria num elevado risco, na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

VIII – Encarregado da proteção de dados – Data *Protection Officer*

Outra das novidades deste RGPD é a criação da figura do Encarregado de Proteção de Dados (EPD), ou, em inglês, *Data Protection Officer*, também designado por DPO.

O EPD é obrigatório no caso de o tratamento ser realizado por uma autoridade ou organismo público, com excepção dos tribunais no exercício da sua função

jurisdicional; sempre que as actividades principais do responsável pelo tratamento ou do subcontratante consistirem 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, e ainda nos casos em que existam operações de tratamento em grande escala de categorias especiais de dados, nos termos do artigo 9.º, e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º.

Um dos principais problemas na interpretação do RGPD nesta matéria e noutras, como a avaliação de impacto sobre a protecção de dados ou a obrigatoriedade de o responsável pelo tratamento ou o subcontratante designar por escrito um representante seu na União, prende-se exactamente com o conceito de "grande escala".

Neste caso, o conceito será determinante para aferir a necessidade ou não de designar um EPD.

Oral, "grande escala" é um conceito indeterminado, não tendo o legislador da União, no artigo 4.º, adiantado qualquer definição para esse conceito.

O 29WP, a que sucedeu o Comité Europeu para a Protecção de Dados, tentou, nas Orientações sobre os encarregados a proteção de dados (EPD), adotadas em 13 de dezembro de 2016 e revistas em 5 de abril de 2017, dar o seu contributo para a densificação deste conceito, prometendo ainda mais intervenção para o futuro, mas o certo é que não conseguiu sanar todas as dúvidas suscitadas em torno desta noção.

De facto, apenas recomendou que, para aferir o conceito de "grande escala" deverão ser tomados em consideração vários factores, entre eles o número de titulares de dados afetados, quer o número em concreto, quer em percentagem da população em causa, o volume de dados e/ou o alcance dos diferentes elementos de dados objecto de tratamento, a duração, ou permanência, da actividade de tratamento de dados, bem como o âmbito geográfico da actividade de tratamento.

O 29WP ainda tentou exemplificar vários tratamentos de dados que considera incluir-se no conceito de grande escala, sendo eles:

- o tratamento de dados de doentes no exercício normal das actividades de um hospital;
- o tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem);

- o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços;
- o tratamento de dados de clientes no exercício normal das actividades de uma companhia de seguros ou de um banco;
- o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca;
- o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet.

Por outro lado, considerou que não constituem tratamento de grande escala, no seguimento do Considerando n.º 91 do RGPD, por exemplo, o tratamento de dados de doentes pacientes por um médico, bem como o tratamento de dados pessoais relacionados com condenações penais e infrações realizado por um advogado.

O Considerando n.º 91 é, aliás, digno de ressalva, ou melhor, a sua versão portuguesa, visto que dispõe o seguinte: *"O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, **hospital** ou advogado"* (destaque e sublinhado nosso). Ora, a referência a "hospital" não é sequer uma tradução errada, mas antes uma verdadeira invenção do tradutor português. A versão inglesa dispõe que *"The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer"*. Ou seja, em nenhum lugar, a não ser na versão portuguesa, se encontra a menção a qualquer hospital neste Considerando. Foi pena a rectificação publicada em 23 de Maio de 2018 não ter corrigido este erro crasso.

O EPD poderá ser partilhado entre empresas do mesmo grupo, mas apenas se este estiver facilmente acessível a partir de cada estabelecimento. Também poderá ser nomeado um EPD para várias autoridades ou organismos públicos, tendo em conta a respectiva estrutura organizacional e dimensão.

A pessoa que for nomeada para este cargo deverá ser designada com base nas suas qualidades pessoais, bem como nos seus conhecimentos especializados no domínio do direito e das práticas de protecção de dados, e na sua capacidade para realizar, em concreto, as suas funções.

Apesar desta redacção parecer ser inócua, pois para cada cargo deverá sempre ser escolhida a melhor pessoa com base nas suas competências, na verdade esta referência consubstancia a importância da posição do EPD para o legislador europeu, e do cuidado que deve existir na sua escolha. Com efeito, o EPD assume uma posição dentro da estrutura do responsável pelo tratamento, no que à proteção de dados diz respeito, de extrema importância e independência. Note-se, por exemplo, que o responsável pelo tratamento e o subcontratante devem assegurar que este não recebe instruções relativamente ao exercício das suas funções, não podendo ser destituído, nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. Também não respeita qualquer hierarquia nestas matérias, já que tem a obrigação de informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

Por este motivo, o artigo 38.º, n.º 6 prescreve que, apesar de o EPD poder exercer outras funções ou atribuições, a verdade é que essas funções e atribuições não podem resultar num conflito de interesses. O que significa, uma vez mais recorrendo à Opinião do 29WP sobre o EPD, "*que não pode exercer um cargo dentro da organização que o leve a determinar as finalidades e os meios do tratamento de dados pessoais. Devido à estrutura organizacional específica de cada organização, este aspeto deve ser apreciado caso a caso. Regra geral, os cargos suscetíveis de gerar conflitos no seio da organização podem incluir não só os cargos de gestão superiores (por exemplo, diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático), mas também outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento. Além disso, pode igualmente surgir um conflito de interesses se, por exemplo, um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados"*. Nesta última parte, o 29WP parece afastar a possibilidade de o EPD ser o advogado que presta assistência jurídica ao responsável pelo tratamento de dados.

Pese embora nada impeça que o EPD seja um trabalhador do responsável pelo tratamento, é necessário acautelar a independência, o que pode levantar alguns problemas no âmbito de uma relação caracterizada pela subordinação jurídica do trabalhador perante o empregador.

Talvez no contexto de uma comissão de serviço, esta independência possa ser assegurada, ainda que a mesma não possa cessar em virtude do exercício das funções de EPD. Já temos mais dificuldades em aceitar o exercício destas funções, com independência, ao abrigo da mobilidade funcional, prevista no artigo 120.º do Código do Trabalho.

As funções do EPD abrangem a informação e aconselhamento do responsável pelo tratamento e dos trabalhadores que tratem os dados, sobre as suas obrigações nos termos do RGPD, bem como o controlo das políticas do responsável pelo tratamento relativas à protecção de dados, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e nas auditorias correspondentes. Também integram as suas funções do EPD emitir parecer relativamente às avaliações de impacto e ser o ponto de contacto entre a autoridade de controlo e o responsável pelo tratamento.

IX – Códigos de conduta e certificação

Com o intuito de apoiar os responsáveis pelo tratamento no cumprimento do RGPD, este prevê a criação de códigos de conduta, bem como a certificação em matéria de protecção de dados.

Assim, dispõe o RGPD que os Estados-Membros, as autoridades de controlo, o Comité e a Comissão podem promover a elaboração de códigos de conduta destinados a contribuir para a correta aplicação, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.

Além das entidades referidas, também as associações e outros organismos representantes de categorias de responsáveis pelo tratamento podem elaborar códigos de conduta, a fim de especificar a aplicação do RGPD.

Até ao momento, os únicos códigos de conduta publicados são códigos de conduta elaborados por algumas associações profissionais, não tendo sido ainda aprovado qualquer código de conduta pela CNDP.

O RGPD prevê ainda que as mesmas entidades acima referidas possam promover a criação de procedimentos de certificação em matéria de protecção de dados, bem como de selos e marcas de protecção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento.

Tal medida seria importante para o controlo do tratamento de dados, não fosse ser bizarramente inócua, sob o ponto de vista do responsável pelo tratamento. Isto porque o n.º 4 do artigo 42.º prevê que a certificação prevista **não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do RGPD.**

Ou seja, quer isto dizer que um qualquer responsável pelo tratamento poderá ser o mais diligente possível, incluindo ver certificadas as suas operações de tratamento pela entidade que o respectivo Estado e autoridade de controlo creditou para o efeito e, mesmo seguindo todas as recomendações dessa entidade, se a autoridade de controlo entender não existir conformidade com o RGPD, a certificação não atenua a responsabilidade do responsável pelo tratamento.

Tal norma poderá, por esse motivo, estar viciada de inconstitucionalidade, violando os princípios da igualdade e proporcionalidade.

X – Regime Sancionatório

Uma das justificações da acentuada preocupação e, em alguns casos, diríamos até pânico, sentidos pelos agentes económicos em relação ao RGPD nos últimos meses está, sem dúvida, relacionada com o seu gravoso regime sancionatório.

De facto, um regime sancionatório com coimas que poderão ascender a 20 000 000 de euros, ou 4% do volume de negócios anual, consoante for o mais elevado, não é uma realidade que quer o cidadão comum, quer as empresas, estejam habituados.

O RGPD abre a possibilidade, que, aparentemente, o Estado Português aproveitará, apesar de muito criticada pela nossa autoridade de controlo, de os Estados isentarem as autoridades e organismos públicos de qualquer coima. Isto porque existiam alguns países, como a Dinamarca e a Estónia, que não previam a aplicação de um regime sancionatório ao abrigo da Directiva agora revogada, o que nunca foi o caso de Portugal, que sempre sancionou, indiferenciadamente, quer as autoridades públicas, que

as privadas. Para além de poder consubstanciar uma violação do princípio da igualdade, nos termos do artigo 13.º da CRP, representará, sem dúvida, um retrocesso na protecção de dados pessoais esta abordagem distinta ao sector privado e ao sector público, em especial, porque este último é maior responsável pelo tratamento dados pessoais em larga escala.

De salientar que a "isenção" de sanções não tem por consequência directa a não existência de qualquer sanção, seja para organismos públicos, seja para privados. Isto porque as coimas não são as únicas sanções possíveis. De facto, poderão existir outras sanções definidas pela autoridade de controlo, que podem ser quer substitutivas, quer complementares à coima. Essas sanções, ao contrário das coimas, que estão definidas no artigo 83.º do RGPD, devem ser determinadas pelos Estados, de acordo com o artigo 84.º, devendo ser efectivas, proporcionais e dissuasivas de comportamentos contrários ao Regulamento.

De todo o modo, será de esperar que a CNPD, na aplicação das coimas previstas no RGPD, assuma uma atitude sensata, que tenha em atenção a realidade dos agentes económicos e o contexto económico nacional, sempre com obediência ao princípio da proporcionalidade e aos princípios enformadores do regime contraordenacional português, que não foram derrogados pelo RGDP.

XI – Conclusão

Em suma, o RGPD é responsável por uma alteração transversal no paradigma do tratamento dos dados.

Por um lado, há um aumento de deveres que impendem sobre o responsável pelo tratamento, aliado à alteração das competências das autoridades de controlo, que abandonaram o controlo prévio a que nos habituaram para assumir uma posição fiscalizadora de cumprimento do RGPD.

Por outro lado, são reconhecidos aos titulares dos dados um conjunto de direitos destinados a promover uma efectiva protecção de dados.

A aplicação do RGPD, a partir dia 25 de Maio de 2018, não marca, em nossa opinião, o fim do tratamento de dados.

Assinala antes o início de uma era de maior consciência e controlo, por parte de todos, no que aos dados pessoais diz respeito, cujo êxito em muito dependerá da intervenção pedagógica e moderada das autoridades de controlo.

Sónia de Carvalho
Advogada

Marcos Tavares Pinho
Advogado

Rua de Vilar, nº 235 6º Esquerdo (Edifício Scala) 4050 – 626 Porto
Telef.: 22 607 607 0
Fax: 22 607 607 9
email: geral@mcsc.pt

WWW.MCSC.PT