CIP
CONFEDERAÇÃO EMPRESARIAL DE PORTUGAL

Proposta de Lei n.º 120/XIII que assegura a execução, na ordem jurídica interna, do 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

– Crítica da CIP –

A Proposta da Lei n.º 120/XIII (doravante PL) que deu entrada no Parlamento diverge, em alguns domínios, e de forma significativa, do projeto objeto de consulta no âmbito do Conselho Nacional de Consumo, e sobre o qual a CIP já se pronunciou.

Por outras palavras, a PL acolheu várias sugestões apresentadas pela CIP.

Não obstante a evolução de cariz positivo, a PL apresenta algumas soluções criticáveis ou que suscitam necessário esclarecimento.

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
Ent.ª 600845
Proc.º 517 07/05/2018

Vejamos.

1.

O preâmbulo da PL apresenta, entre outras, uma passagem que merece comentários.

A passagem em causa é a seguinte:

"O paradigma que esteve subjacente ao legislador europeu foi o das grandes multinacionais que gerem redes sociais ou aplicações informáticas à escala global, envolvendo a recolha e utilização intensivas de dados pessoais.

Por esse motivo, algumas das soluções jurídicas que foram plasmadas para esse universo

revelam-se por vezes desproporcionadas ou mesmo desadequadas para a generalidade do tecido empresarial nacional e para a Administração Pública, aos quais o RGPD, todavia, também se aplica.

Assim, do trabalho de avaliação de impacto já realizado, conclui-se que a aplicação deste regulamento resultará em encargos administrativos elevados, que em muitos casos não se encontram suficientemente justificados pelos benefícios obtidos com o novo regime de proteção de dados pessoais relativamente ao regime atual." (sublinhados nossos).

Ora, do supratranscrito, constata-se que o legislador nacional compreendeu, por um lado, a complexidade da matéria, e, por outro lado, que o Regulamento implicará elevados encargos para as empresas, os quais devem necessariamente ser minimizados ao máximo dentro da margem de adaptação concedida aos Estados-Membros.

Trata-se de uma evolução que não pode deixar de ser sublinhada de forma positiva.

Por outro lado, faz-se referência ao "*trabalho de avaliação de impacto já realizado*".

A CIP desconhece por completo tal trabalho de avaliação.

Aliás, é de sublinhar que, no dia 21 de março de 2018, representantes da Medida "Quanto custa", que visa medir o impacto das iniciativas legislativas aprovadas pelo Governo na vida das pessoas e na atividade das empresas, contactaram a CIP com vista à colaboração desta Confederação no apuramento dos impactos, sendo que tais trabalhos, ao que podemos apurar, ainda se encontram numa fase muito preliminar.

Assim sendo, questiona-se: Que trabalho já foi desenvolvido ?

Quais os resultados desse mesmo trabalho ?

Que reflexo tiveram tais resultados na PL.

Como a CIP já teve oportunidade de o referir, o apuramento rigoroso e cabal dos múltiplos impactos suscetíveis de terem lugar, particularmente junto das PME, impõe-se.

Na perspetiva da CIP, muitas das medidas previstas terão um custo muitíssimo relevante, o qual não pode ser omitido ou negligenciado, para a esmagadora maioria das empresas, ressaltando, como é obvio, a estrutura empresarial existente: micro, pequenas e médias empresas.

Ora, se bem que se observe sinais económicos positivos, verifica-se que a retoma ainda não se encontra solidamente sustentada.

Neste quadro, quaisquer medidas que comprometam a competitividade das empresas, devem ser objeto de profunda reflexão e análise de impacto, por forma a não "deitar por terra" tudo o que, desde o início da crise em finais de 2008 e até ao presente momento, se foi construindo e desenvolvendo.

Na perspetiva da CIP, o objetivo principal do nosso País continua a passar por procurar respostas destinadas a promover o crescimento económico e, por essa via, a criação de emprego.

A aposta em manter e aumentar o emprego deve, pois, revestir caráter central e estar presente em qualquer discussão.

Neste quadro, o que se devia preconizar e priorizar é a exponenciação dos fatores que, de forma significativa, contribuíram e são suscetíveis de contribuir para reforçar os indicadores económicos e sociais positivos já observados.

Adiante-se, desde já, os seguintes custos de contexto identificados.

A proliferação de suportes legais, a incerteza quanto aos conceitos genéricos e indeterminados, as nuances estabelecidas na PL relativamente ao RGPD, vai fazer aumentar a litigância na comunidade empresarial, representando um elevadíssimo custo

do contexto, em particular para as PME (com menos recursos), atendendo ao valor elevado das custas judiciais, acrescidas de honorários (além da entropia causada no regular funcionamento da empresa), a que se junta o agravamento da morosidade da justiça.

O princípio da auto-responsabilização (accountability) imposto no RGPD obriga as empresas a efetuar uma avaliação de impacto complexa, morosa e onerosa para aferir dos requisitos do artigo 35.º n.º 1 RGPD, configurando tal exigência um elevado custo do contexto, mais uma vez particularmente gravosa para as PME, que se debatem com uma maior escassez de meios.

A isenção das obrigações de registo (artigo 30.º do RGPD) para as empresas com menos de 250 trabalhadores pode cair caso, na avaliação de impacto, a entidade prestadora desse serviço venha a determinar que existe risco para os direitos e liberdades dos titulares, atividade essa – de registo, burocrática – consumidora de tempo e recursos, elevada à categoria de custo de contexto e particularmente gravosa para as PME.

2.

Por outro lado, perante a aproximação do fim do período de transição de 2 anos do regulamento europeu, em 25 de maio próximo, teria sido exigível, que o regulamento nacional já tivesse sido concluído, dando mais tempo de adaptação a empresas e Estado nas matérias deixadas em aberto pelo regulamento europeu.

A solução ora proposta para a entrada em vigor do diploma é lamentável e manifestamente criticável.

Veja-se que o artigo 64.º (Entrada em vigor) prevê que a *"presente lei entra em vigor no dia seguinte ao da sua publicação."*

A entrada em vigor no dia seguinte ao da publicação da Lei revela uma total insensibilidade, senão mesmo desrespeito, para com as empresas.

De facto, para além de não relevar a complexidade da matéria, o legislador não concede qualquer margem, em termos temporárias, para a necessária adaptação das empresas.

Diga-se, aliás, que só falta que a CNPD comece a fiscalizar a aplicação da lei dois dias após a entrada em vigor do diploma.

É certo que o RGPD entra em vigor no dia 25 de maio.

Mas também é certo que as empresas não podem ser responsabilizadas pela manifesta inépcia do legislador.

Estamos, assim, mais uma vez, perante um exemplo claro onde o legislador compromete a competitividades das empresas.

3.

Na perspetiva da CIP, tendo em conta i) a especial complexidade da matéria – julga-se que ninguém o desmente –; ii) os ainda baixos níveis de qualificação da população portuguesa; iii) e a dimensão da estrutura empresarial nacional, impõe-se, também, com urgência, o desenvolvimento de ferramentas informáticas (vg.: check lists), simples na sua leitura e pragmáticas na resposta às novas obrigações, que apoiem as empresas, nomeadamente as PME.

Tal aposta, impõe-se se queremos assegurar uma transição adequada de regimes.

Veja-se, a título de mero exemplo, o trabalho que tem sido desenvolvido por parte da Autoridade Espanhola, a qual já disponibiliza no seu Portal uma ferramenta eletrónica.

Na perspetiva da CIP, a CNPD tem obrigatoriamente de seguir igual ou semelhante procedimento por forma a auxiliar as empresas.

Em síntese, é perspetiva desta Confederação, que o sucesso na aplicação do novo regime passa sobremaneira pelo papel da CNPD, quer na divulgação de informação quer na disponibilização de ferramentas que auxiliem as empresas.

4.

Por outro lado, também numa perspetiva geral, é necessário que fique bem claro o seguinte: Na perspetiva da CIP, face ao peso, em termos burocráticos e financeiros, associados à implementação do RGPD, é inadmissível que a possibilidade de ajustamentos conferida pelo RGPD ao legislador nacional sirva para agravar, ainda mais, tais encargos.

Pelo contrário, é perspetiva desta Confederação, que a intervenção do legislador através da presente PL deve ter por objetivo, quanto possível, o de aligeirar a multiplicidade de obrigações que ora se intenta imputar às empresas, bem como eventuais dúvidas interpretativas originadas pelo RGPD.

Aliás, outra solução não é concebível, quando a própria "Exposição de motivos" reconhece que do RGPD decorrem "*encargos administrativos elevados*".

5.

A Agenda Digital, uma das sete iniciativas no âmbito da estratégia «Europa 2020» para um crescimento inteligente, sustentável e inclusivo da União Europeia, entre outras vertentes viradas para o seu objetivo principal, propunha um pilar de garantia de uma maior segurança em linha, em particular para os utilizadores mais vulneráveis – os consumidores que disponibilizam dados.

É no desenvolvimento deste pilar garantístico que se opta pela criação de um novo regulamento de proteção de dados em vez do desenvolvimento e alteração da Diretiva 95/46/CE.

Em lado nenhum se encontram argumentos para se defender que a segurança dos dados pessoais recolhidos e existentes são mais vulneráveis nas empresas do que no Estado e nos organismos que ele superentende.

Porém, reconhecendo o legislador comunitário que o Estado é uma entidade abstracta e aglutinadora de muitas realidades distintas onde poderia fazer sentido haver uma exceção em algumas matérias, nomeadamente no regime de aplicação de coimas, previu

essa possibilidade no artigo 83.º n.º 7 do RGPD, nos seguintes termos: "*Sem prejuízo dos poderes de correção das autoridades de controlo nos termos do artigo 58.º, n.º 2, os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território*".

Ora, ao abrigo desta norma cuja redação indicia claramente o seu carácter excecional, o legislador português aproveitou e consagrou uma exceção geral para todas as entidades públicas (v. artigo 49.º n.º 1 do Regulamento 2016/679) – não há aplicação de coimas às entidades públicas, o que constitui, efetivamente, um fortíssimo incentivo ao relaxe e à descredibilização das entidades públicas.

Por outro lado, as empresas e os cidadãos, nunca verão as entidades públicas serem penalizadas pelas não conformidades, quando geralmente se espera que as entidades publicas sirvam de exemplo ao resto da economia.

Face ao exposto, a exceção prevista para o setor público na aplicação de contraordenações é absolutamente inaceitável.

Os cidadãos têm o direito de ver os seus dados protegidos independentemente de ser o Estado ou outra organização a potencialmente os violar.

De resto, historicamente, a privacidade e proteção de dados pessoais revela-se mais vulnerável e perigosamente ameaçada por poderes públicos.

O Estado deve dar o exemplo.

É inaceitável que exija a outros aquilo que se mostra incapaz de cumprir.

6.

Relativamente ao artigo 2.º, consideramos que esta norma só faz sentido se for dirigida aos postos consulares, devendo, nesse caso, a redação ser mais clara. Se a ideia é a de aplicar a legislação portuguesa a qualquer entidade, será uma imposição muito onerosa,

pois é difícil a identificação da nacionalidade do titular dos dados, assim como a inscrição nos serviços consulares portugueses, caso tenha nacionalidade portuguesa.

Sem prejuízo do suprarreferido, cumpre clarificar divergência entre as versões nos diferentes idiomas: "*residam*" vs "*que se encontrem*".

Independentemente da escolha, a aplicação dos requisitos do regulamento será muito provavelmente feita de forma generalizada.

7.

O artigo 4.º nº 1 refere "*A CNPD (...) que funciona junto da Assembleia da República.*".

A menção e o seu alcance deveriam ser melhorados.

8.

No âmbito do artigo 6.º (Atribuições e competências) e atendendo a que o cumprimento de códigos de conduta ou de procedimentos de certificação aprovados pode ser utilizado como elemento para demonstrar o cumprimento das obrigações/garantias suficientes e pode ser considerado na avaliação do impacto de operações, entendemos pertinente incluir de forma expressa nas atribuições e competências da autoridade de controlo nacional a publicação de listas das entidades que cumprem códigos de conduta aprovados e que obtiveram certificação aprovada e/pu a quem foram atribuídos selos e marcas de proteção de dados, para que a aplicação prática desse cumprimento nos aspetos referidos seja feita de forma objetiva e transparente.

Por outro lado, relativamente à alínea d), a PL deve referir expressamente a data até à qual a CNPD tem de publicitar pelo menos a lista com os tratamentos obrigatoriamente sujeitos à avaliação do impacto sobre proteção de dados, data essa que nunca poderia ser posterior a 25 de maio de 2018.

Verifica-se, no entanto, na prática, que tal prazo não será exequível.

9.

Relativamente ao artigo 7º (Avaliações Prévias de Impacto) entendemos que este artigo é redundante com o que já estabelece o RGPD.

Por outro lado, e no que diz especificamente respeito ao nº 3 deste art.º 7º, referente à publicitação das listas de tipos de tratamentos de dados que implique, ou não, uma avaliação prévia de impacto, não esclarece qualquer tipo de mecanismo de notificação de futuras alterações às mesmas, o que poderá implicar que os responsáveis pelos tratamentos não tenham conhecimento das mesmas.

Isto, bem como o provável caráter não exaustivo das listas, poderá gerar alguma incerteza, pelo que sugerimos que este nº 3, também preveja uma obrigatoriedade de publicitação das alterações a essas listas com um pré-aviso razoável, de forma a permitir que os responsáveis pelos tratamentos abrangidos tenham tempo útil para se adaptar.

Por outro lado, cumpre salientar que a redação da norma em análise não é clara e deveria ser fundida com o artigo 6.º, n.º 1, alínea c) para garantir uma interpretação rigorosa e coerente do aplicador.

O RGPD, no artigo 35.º, n.º 4 e 5 dispõe que a CNPD "*elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados*" (v. n.º 4, a chamada "black list") e "*pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto*" (v. n.º 5, a chamada "white list").

O legislador português, de forma confusa, optou por distribuir estas duas obrigações em duas normas diferentes: no artigo 6.º, n.º 1, alínea c) (para a "black list") e no artigo 7.º (para a "white list").

10.

O disposto no n.º 4 do artigo 8.º não é claro.

Não se compreende se prevalece o dever de segredo, ou precisamente o contrário, ou seja, o dever de colaboração. Em princípio, deverá pretender-se que prevaleça o dever de segredo. Para esse efeito, deverá adotar-se uma redação mais clara.

11.

Relativamente ao artigo 9.º (Disposição geral), deverá reverter-se para a redação constante noutras versões/idiomas do RGPD, em que se refere "*conhecimentos especializados das práticas e da legislação de proteção de dados*".

12.

O artigo 10.º (Dever de sigilo) visa estabelecer o seguinte:

"De acordo com o disposto no n.º 5 do artigo 38.º do RGPD, o encarregado de proteção de dados está obrigado ao dever de sigilo durante o exercício de funções, mantendo-se tal dever após o termo das mesmas. (sublinhado nosso).

Por um lado, ficam por esclarecer quais as implicações exatas do dever de sigilo profissional imposto ao Encarregado da Proteção de Dados ("DPO").

Pode um DPO escusar-se a depor em tribunal sobre os factos abrangidos pelo segredo profissional (aqueles de que tome conhecimento no exercício de funções) ?

Por outro lado, a manutenção do dever de sigilo, sem qualquer limite temporal, após o exercício das funções, o qual não se encontra previsto no RGPD, deve ser objeto de ponderação, tendo em conta, nomeadamente, a natureza e importância dos dados.

13.

A utilização do conceito "código malicioso" na alínea b) do artigo 11.º (Funções do encarregado de proteção de dados) é indecifrável para o intérprete e não faz sentido do ponto de vista prático, uma vez que um incidente de segurança pode ter origens muito distintas e vai muito além da deteção de código malicioso, algo que, inclusive, poderá requerer um perfil técnico que a grande maioria das pessoas que lidam com dados pessoais não tem.

Assim, propõem-se substituir o conceito de "responsável de segurança" por "responsável pelo tratamento" e generalizar "código malicioso" para "qualquer indício de violação de dados pessoais".

14.

O n.º 3 do artigo 14.º (Acreditação e certificação) não é claro porquanto parece excluir a CNPD dos organismos de certificação o que resulta, inequivocamente, do artigo 42.º, n.º 5 e 43.º do RPGD.

15.

Em primeiro lugar, no âmbito da alínea a) do artigo 15.º (Funções do encarregado de proteção de dados), questiona-se: As auditorias não programadas quando é que são realizadas ?

Em segundo lugar, um dos aspetos que tem assumido grande relevância nas últimas décadas é o da preservação da informação, que cruza vertentes tão distintas como as de formatos, dos suportes e dos sistemas de gestão de informação de arquivo. Um dos riscos mais significativos associados à digitalização da economia é o da preservação digital, que decorre entre outros fatores da obsolescência tecnológica, que se verifica em ciclos cada vez mais curtos e pode, de forma silenciosa, levar à perda de volumes significativos de informação crítica pata a salvaguarda de direitos e obrigações.

Pela sua relevância, considera-se oportuno introduzir de forma expressa este aspeto na PL.

Em terceiro lugar, não se compreende o sentido e alcance da alínea c).

16.

O artigo 15.º (Códigos de conduta) refere que "*Compete à CNPD fomentar a elaboração (...)*"

Questiona-se: O que significa a expressão "*fomentar*" ?

Por outro lado, é igualmente de sublinhar que à CNPD também cabe aprovar os referidos Códigos, de acordo com o n.º 5 do artigo 40.º do RGPD.

17.

Relativamente aos menores (v. artigo 16.º), sublinha-se que a chave digital móvel só está disponível a partir dos 16 anos de idade, em conformidade com a Lei n.º 37/2014, de 26 de junho, o que é incompatível com o estabelecimento da idade mínima de 13 anos.

Por outro lado, é ainda de sublinhar o seguinte.

A PL prevê no artigo 16.º que o tratamento de dados pessoais de menores, com base no consentimento destes e relativo à oferta direta de serviços da sociedade de informação, é lícito desde que os menores já tenham completado os treze anos de idade.

Ora, contrariamente ao teor do n.º 1 do artigo 16.º, o artigo 8.º do RGPD limita a licitude deste tratamento à idade de 16 anos.

O que o RGPD vem determinar é que, atendendo à diversidade das soluções já previstas nos vários ordenamentos jurídicos sobre a incapacidade/capacidade dos menores, os Estados-Membros podem dispor no seu direito uma idade inferior para este efeito, desde que essa idade não seja inferior a 13 anos.

No ordenamento jurídico português, de acordo com o disposto no Código Civil, o legislador determina, como regra geral, a incapacidade para o exercício de direitos de quem não tiver ainda completado dezoito anos de idade (cfr. artigos 122.º e 123.º do Código Civil).

Acresce que, de uma leitura sistemática ao Código Civil verifica-se que quase todas as exceções previstas para a regra geral de incapacidade de menores de 18 anos reportam-se à idade do menor de, pelo menos, dezasseis anos (cfr. artigos 127.º, 1850.º, 1886.º, 1612.º, etc.).

Salienta-se que as próprias regras previstas para o consentimento do titular dos dados constantes no art.º 7.º do RGPD, são bastante restritas. O consentimento deve ser realizado por escrito, ser claro, de fácil acesso, numa linguagem clara e simples e de fácil compreensão, de uma forma que o referido consentimento se distinga claramente de qualquer outro assunto.

Ao prever o consentimento das crianças a partir dos 13 anos de idade, a PL, além de não acautelar a segurança dos menores no acesso aos meios informáticos e na sociedade da informação, contraria aquilo que é a visão do legislador português relativamente à capacidade dos menores, prevista no Código Civil.

Sugere-se a alteração do teor deste artigo, aumentando a idade do consentimento do menor para determinar a licitude do tratamento dos seus dados pessoais relativos à oferta direta de serviços da sociedade de informação para os 16 anos.

Sem prejuízo do exposto, entendemos que um responsável pelo tratamento no setor da saúde tem de ter liberdade para estabelecer uma exigência mais elevada na obtenção do consentimento de crianças, nomeadamente definindo a idade mínima de 16 anos para que os utilizadores do seu serviço online possam, validamente, consentir no tratamento dos seus dados pessoais (incluindo dados relativos à saúde) na plataforma.

18.

Relativamente à proteção de pessoas falecidas, ao conceder-se os direitos de acesso, retificação dos dados sensíveis (ou das categorias especiais de dados) do falecido aos herdeiros poder-se-á estar a violar a privacidade e a memória do falecido, na medida em que este pode ter pretendido, em vida, não divulgar determinados dados mesmo relativamente aos seus herdeiros.

Nesse sentido, não se protege da melhor forma a memória do falecido ou os seus direitos e aspirações em vida quanto à sua privacidade.

Neste âmbito, a solução prevista na proposta de lei nacional de execução do RGPD espanhola parece mais adequada, ao incluir o seguinte: "*Como excepción, los herederos*

no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley."

Importa clarificar qual a consequência do n.º 2 do artigo 17.º (Proteção de dados pessoas de pessoas falecidas), em particular se implica o cumprimento da obrigação de informação junto dos herdeiros de pessoas falecidas.

O ponto é relevante pois a proteção é dada apenas no contexto de tratamento de dados sensíveis (onde se incluirá o tratamento de investigação clínica) e urge clarificar qual a intenção do legislador.

19.

Relativamente ao artigo 18.º (Portabilidade e interoperabilidade dos dados), sugere-se alinhamento com RGPD 20.1 (que exclui dados não fornecidos pelo titular).

20.

O artigo 19.º reporta-se à Videovigilância.

O tratamento de dados pessoais no contexto da videovigilância para proteção de pessoas e bens é submetido a requisitos específicos pelo artigo 19.º.

Para além dos requisitos constantes do artigo 31.º da Lei nº 34/2013, de 16 de maio, o texto define, nomeadamente, que "*As câmaras, ou outros meios de captação de som e imagem, não podem incidir sobre: a) Vias públicas ou propriedades limítrofes, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel; b) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM; c)O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário; d) O interior de áreas reservadas aos trabalhadores, designadamente vestiários e instalações sanitárias.*".

Ora, não nos parece que a imposição destes requisitos adicionais decorra de uma prerrogativa do Estado português à luz do artigo 23º do RGPD, porquanto não visa limitar o alcance dos direitos dos titulares dos dados à luz do RGPD.

A remissão para a Lei n.º 34/2013, de 16 de maio resolve a dúvida sobre o potencial conflito entre aquela lei e o RGPD.

No entanto, cumpre esclarecer que nem todos os sistemas de videovigilância estão, atualmente, abrangidos pelas regras da Lei n.º 34/2013 de 16 de maio. Esta Lei abrangia apenas as entidades previstas no seu artigo 7.º a 9.º.

A generalidade das pequenas e médias empresas, bem como dos prédios em regime de propriedade horizontal, podem implementar um sistema de videovigilância, sem necessidade de contratar um serviço de segurança privada, ou implementar um sistema de autoproteção. Porém, de acordo com a redação da presente Proposta de Lei, a instalação de um sistema de videovigilância obriga sempre à contratação de um serviço de segurança privado ou à implementação de um sistema de autoproteção. Esta é uma solução extremamente onerosa para a generalidade das empresas e cidadãos, promovendo, de forma desproporcionada, a obrigação de contratação de serviços de segurança privada.

21.

O n.º 2 do artigo 21.º (Prazo de conservação de dados pessoais) refere que "*Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, é lícita a conservação dos dados pessoais.*"

Questiona-se: A conservação é licita até quando ? Até à aplicação do n.º 4 do artigo em análise ?

O RGPD inclui na informação a prestar ao titular, no direito de acesso, na proteção de dados desde a conceção e por defeito (omissão) e no registo de atividades de tratamento a indicação do prazo de conservação ou dos critérios para o determinar.

Neste contexto, entendemos que a impossibilidade de determinação do momento não deverá só por si determinar a conservação permanente dos dados pessoais, mas que deverá determinar apenas a conservação de acordo com os critérios para determinação do prazo e a avaliação que se faça dessa informação.

O n.º5 refere "*Nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 17.º do RGPD findo esse prazo.*".

O RGPD estabelece condições para aplicação do direito ao esquecimento e identifica a sua não aplicação em casos de exercício de liberdade de expressão e de informação, cumprimento de obrigação legal, saúde pública, arquivo, investigação científica ou histórica e fins estatísticos e declaração, exercício ou defesa de um direito num processo judicial.

Caso seja intenção do legislador reforçar a prevalência da obrigação legal (critério legal direto) de guarda da informação, recomendamos no mínimo a inclusão de forma explícita também dos prazos prescricionários das responsabilidades (critério legal indireto), sem prejuízo dos restantes casos referidos no RGPD.

22.

O artigo 23.º (Tratamento de dados pessoais por entidades públicas para finalidades diferentes) suscita os seguintes comentários.

Em primeiro lugar, relativamente ao disposto no nº 1 deste artigo, o mesmo suscita-nos muitas dúvidas em relação à sua conformidade com o que está disposto no RGPD, na medida em que, mesmo para entidades públicas, o tratamento de dados pessoais para finalidades distintas daquelas para os quais foram recolhidos está sujeito a um âmbito especificamente definido no RGPD – em particular, nº 4 do artigo 6º e nº 1 do artigo

23º -, que a presente norma proposta pelo legislador nacional não parece cumprir com a mera remissão para a prossecução do interesse público como fundamento para o tratamento para finalidades distintas.

A alínea g) do n.º 2 do artigo 9.º do RGPD, por exemplo, referido na dita norma, exige um "motivo de interesse público importante", não se bastante com a formulação aqui sustentada pelo legislador nacional.

Em segundo lugar, o nº 2 do artigo 23º parece onerar excessivamente as entidades públicas que troquem dados para finalidades diferentes daquelas que motivaram a recolha.

Com efeito, ao exigir que estas entidades celebrem um "*protocolo, que estabeleça as responsabilidades de cada entidade interveniente*", o legislador parece configurar a relação entre as entidades públicas como sendo de corresponsabilidade pelo tratamento de dados (à luz do artigo 26.º do RGPD) quando, na verdade, cada entidade assumirá a posição autónoma de responsável pelo tratamento relativamente às finalidades prosseguidas por cada uma.

Em segundo lugar, é necessário clarificar que a PL não pretende introduzir limitações à abertura do RGPD sobre o uso secundário dos dados ou tratamentos diferentes dos originais no contexto da investigação científica.

23.

Relativamente ao disposto no n.º 2 do artigo 24.º (Liberdade de expressão e informação), deve haver uma referência expressa, em linha com o espírito do RGPD, à "*liberdade de expressão*" num sentido amplo e não limitada aos campos académicos, artísticos e literários.

Ainda no n.º 2, a formulação parece indicar que a ponderação em causa cabe ao titular dos direitos, enquanto entidade que tem o poder de exercer ou não os direitos ali identificados – "*(...) são exercidos num quadro de ponderação (...)*".

A redação é, assim, equívoca, por não permitir perceber com clareza quem deve concretizar esta ponderação, e por não esclarecer que tal ponderação deve ser feita por quem tem de assegurar o cumprimento dos direitos em causa (julgamos que outra coisa não faz sentido).

24.

O artigo 25.º (Publicação em jornal oficial) é, por um lado, desnecessário, pelo que deve ser eliminado, e, por outro lado, gerador de equívocos no que diz respeito ao seu n.º 4.

O n.º 4 do artigo 25º prevê que "*O direito ao apagamento quanto a dados pessoais publicados em jornal oficial concretiza-se, nas condições previstas no artigo 17.º do RGPD, através da desindexação desses dados pessoais em motores de busca*".

Nos termos do artigo 17º do RGPD, "*o titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada*".

Não se considera que a medida prevista no nº 4 do artigo 25.º seja suficiente para cumprir o previsto no artigo 17º do RGPD.

Desindexar dados pessoais de motores de busca não significa apagá-los. Esta proposta consiste em coartar o direito previsto e deverá ser alterada.

Face ao exposto, o artigo deve ser eliminado sendo o RGPD a norma.

25.

O artigo 28.º tem por epígrafe as "*Relações laborais*".

O n.º 1 do artigo 28.º prevê o seguinte: "*O empregador pode tratar os dados pessoais dos seus trabalhadores nos termos definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo*".

No âmbito do n.º 1 do artigo 28.º questiona-se o seguinte.

Basta invocar o n.º 1 como condição de legitimidade ?

Ou é necessário aditar cada norma da legislação nacional para poder recolher o dado ?

Vejamos um exemplo: Para pedir informação sobre número de dependentes, para efeito de retenção em sede de IRS, é necessário invocar a norma que explica como se aplicam as tabelas de retenção ou é possível fazer referência exclusiva à norma do n.º 1 do artigo 28.º ?

A resposta a esta questão, revela-se, na prática, muito importante.

Diga-se, desde já, que, na perspetiva da CIP, tendo em conta os princípios da adequação e proporcionalidade, da razoabilidade, e da salvaguarda da competitividade das empresas, a mera referência ao n.º 1 do artigo 28.º deve ser suficiente para legitimar o acesso aos dados.

Por outro lado, importa precisar que a referência a "*regimes setoriais*" não diz respeito a setores, mas sim, a matérias, como, no caso anteriormente apontado, ao IRS.

Quanto ao n.º 2, pressupõe-se no mesmo que as atividades de relações laborais se resumem a aspetos contabilísticos relacionados com o processamento salarial.

Existem vários tipos de atividades de natureza técnica, no âmbito das prestações de serviços de gestão de trabalhadores, desde o recrutamento e seleção, formação profissional, gestão de desempenho, segurança e saúde no trabalho.

Estas atividades podem ser asseguradas através de subcontratação de empresas especializadas, mediante contrato de prestação de serviços. Sempre que estes serviços sejam prestados por entidades externas com envolvimento de dados pessoais, devem estar sujeitos às regras de subcontratação do RGPD.

A referência a contabilista certificado parece restringir a possibilidade do âmbito destes serviços, traduzindo uma visão restritiva da realidade.

Ainda relativamente ao princípio geral de não ser aceite o consentimento no âmbito laboral, não se compreende o que se pretende abranger e o significado do conceito utilizado na redação do n. 3 do artigo 28.º - vantagem jurídica, por contraposição com o conceito de vantagem económica.

Por outro lado, os n.ºs 4 e 5 do normativo em análise referem o seguinte:

"4 - As imagens gravadas e outros dados pessoais registados através da utilização de vídeo ou outros meios tecnológicos de vigilância à distância, nos termos previstos no artigo 20.º do Código do Trabalho, só podem ser utilizadas no âmbito do processo penal.
5 - Nos casos previstos no número anterior, as imagens gravadas e outros dados pessoais podem também ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal."

Do supra transcrito parece inferir-se que fica de todo precludida a utilização de imagens e outros dados registados no âmbito do processo disciplinar a menos que a mesma tenha sido também utilizada como prova em processo crime – um entendimento que, em muitas situações, conduziria a verdadeiras aberrações.

De facto, parece exigir-se que as imagens gravadas e outros dados pessoais registados através da utilização de meios tecnológicos de vigilância/controlo à distância tenham de ser utilizadas em processo-crime, antes de o poderem ser em sede de procedimento disciplinar iniciado contra o trabalhador visado.

Se esta solução parece ir ao encontro do entendimento da CNPD na sua Deliberação nº 61/2004 "*Princípios sobre o tratamento de dados por videovigilância*" e do artigo 31º, nº 4 da Lei nº 34/2013, de 16 de maio, existe também uma linha jurisprudencial que tem um entendimento contrário.

No seu Acórdão de 8 de outubro de 2014, o Tribunal da Relação de Lisboa entendeu que "*É de aceitar as imagens captadas por sistema de videovigilância como meio de prova em processo disciplinar e na subsequente ação judicial em que se discuta a aplicação de sanção disciplinar, mormente o despedimento, desde que sejam observados os pressupostos que decorrem da legislação sobre a proteção de dados e concomitantemente se conclua que a finalidade da sua colocação não foi exclusivamente a de controlar o desempenho profissional do trabalhador. Num quadro circunstancial assim apurado, o trabalhador não merece – nem a lei lhe confere - maior proteção do que aquela que é conferida aos demais cidadãos e, logo, o meio de prova é lícito e admissível*".

No caso vertente, não teria havido qualquer processo-crime intentado contra o titular dos dados.

Assim, entendemos que a regra de precedência de processo-crime elencada não tem razão de ser e deve ser eliminada.

Atente-se, igualmente, ainda no contexto da utilização de imagens gravadas e dados recolhidos através de meios de vigilância à distância para fins disciplinares, que a norma pode ser interpretada no sentido de que a utilização fica dependente do desfecho do processo crime.

Ora, atendendo ao prazo de prescrição do procedimento disciplinar, essa interpretação conduziria à inutilidade da norma.

Ainda que se admitisse que a utilização dos dados em processo disciplinar estivesse dependente de apresentação de queixa-crime, deverá ser sempre clarificado que essa utilização poderá ser feita sem ter de se aguardar pelo desfecho do processo criminal, sob pena de inutilidade da norma.

No que diz respeito ao n.º 6, o conceito de dados biométricos previsto na Proposta de Lei não parece coincidente com o conceito constante do RGPD.

De acordo com o artigo 4.º n.º 14 do RGPD, são dados biométricos aqueles que "*...permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos*".

Mais, de acordo com o artigo 9.º do RGPD só constituem categorias especiais de dados os dados biométricos que inequivocamente identificam o seu titular.

No entanto, a Proposta de Lei estabelece que o tratamento de dados biométricos só é considerado legítimo para o controlo de assiduidade e para o controlo de acessos às instalações do empregador.

A generalidade dos sistemas de registo de tempos de trabalho e de controlo de acessos registam uma representação digital (template), e não uma amostra biométrica passível de ser reproduzida. Aliás, em teoria, o mesmo registo pode representar mais do que um utilizador. Este é o pressuposto da deliberação da CNPD de 26 de fevereiro de 2004.

Esta redação pode induzir em erro relativamente ao conceito de dados biométricos para efeitos de proteção de dados pessoais, bem como aos requisitos técnicos a que devem obedecer os equipamentos de controlo de assiduidade e de controlo de acessos.

Por outro lado, relativamente aos ns.º 7 e 8, julgamos depreender-se que as empresas em relação de domínio de grupo só podem transferir dados de colaboradores entre si em caso de expatriação ou missão.

Ora, se é este o alcance da lei, põe em causa todas as estruturas de serviços partilhados existentes em multinacionais para processamento de salários, dados relativos a desenvolvimento de carreira internacional, formação, etc.

Por outro lado, não se coaduna com o disposto no Regulamento, no que respeita à possibilidade dos grupos empresariais estabelecerem as sua regras vinculativas que permitem a transferência de dados entre o grupo, contrariando ainda o disposto no Considerando 48 do Regulamento que refere que "*os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo*

central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes e funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro, mantêm-se inalterados.", de acordo com o qual bastará haver acordos intragrupo, ou as regras vinculativas às empresas, para transferir dados de colaboradores.

Face ao exposto e no nosso entendimento, estas disposições deveriam ser eliminadas da Proposta por:

- Não estarem de acordo com o espírito do RGPD e
- Trazerem graves entraves ao funcionamento das empresas multinacionais que estão dotadas de estruturas de serviços partilhados que têm como objeto todas as atividades relacionadas com colaboradores do Grupo e que, naturalmente, envolvem o acesso e processamento de dados pessoais.

26.

A menção no n.º 2 do artigo 29.º (Tratamento de categorias especiais de dados pessoais) a "*encarregado de proteção de dados*" é desnecessária, por já se mostrar coberta ao abrigo do disposto no artigo 10º.

27.

A norma prevista no artigo 30.º não concretiza o princípio genérico constante do RGPD.

Na perspetiva da CIP o artigo deve ser eliminado.

Existindo uma norma direcionada a este tema, deveria definir requisitos de segurança mais específicos.

28.

O artigo 31.º (Tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos) suscita os seguintes comentários.

Em relação ao n.º 1 do artigo 31.º sugere-se eventual revisão da redação de forma a que se possa prever que os mecanismos de pseudonomização e anonimização sejam implementados quando os fins sejam igualmente alcançados, e desde que tais mecanismos sejam tecnicamente possíveis e não sejam desproporcionalmente onerosos, conforme veiculado pelo RGPD.

No n.º 4 do artigo em análise, é expressamente previsto que em caso de investigação científica são aplicáveis as regras gerais sobre consentimento previstas no RGPD, considerando-se que o mesmo pode abranger diversas áreas de investigação, devendo ser respeitados os padrões éticos reconhecidos pela comunidade científica.

Na perspetiva da CIP, não devem ser introduzidas restrições adicionais no que respeita ao consentimento obtido para investigação científica e que deve ser admitido um consentimento amplo (cfr. Considerando 33 do RGPD) para utilização de dados relativos à saúde para finalidades primária e secundária (cfr. Considerando 50 do RGPD).

Não parece, assim, que tenham sido introduzidas limitações à amplitude do consentimento (Considerando 33 do RGPD), contudo, não podemos deixar de ter presente a definição de Consentimento Informado constante na Lei da Investigação Clínica que exige informação "*sobre a natureza, o alcance, as consequências e os riscos do estudo*", pelo que importa clarificar que esta exigência não obsta à obtenção de consentimento válido nos termos do n.º 4 do artigo 31.º e que as Comissões de Ética não terão uma interpretação mais restritiva do que a CNPD sobre a possibilidade de um consentimento amplo (que podem ser mais conservadoras e impedir o uso secundário dos dados).

Na perspetiva da CIP, é importante que fique expressamente definido que o legislador ao optar pela expressão "*o mesmo pode abranger diversas áreas de investigação*" está a optar por consentimento amplo.

29.

O artigo 33.º (Responsabilidade civil) suscita os seguintes comentários.

A primeira parte do artigo 33.º, n.º 1, contempla os casos de responsabilidade civil delitual (porque fundada no "tratamento ilícito de dados") e a segunda parte prevê as possibilidades em que essa mesma responsabilidade se funda em violações de normas em matéria de proteção de dados pessoais.

Trata-se, ainda, de responsabilidade civil delitual, mas em que o facto ilícito se reconduz à violação de normas que visam a proteção de dados pessoais.

Note-se que, neste segundo grupo de situações, em nosso entender, e em função do disposto no artigo 483.º, n.º 1, segunda parte, do Código Civil, para que haja lugar a indemnização é necessário que a norma violada seja uma norma estabelecida no interesse daquele que invoca o direito à indemnização e que haja suportado o dano na sua esfera jurídica.

Neste sentido, haverá que interpretar o artigo 33.º, n.º 1, segunda parte, no sentido de aí só poderem estar em causa normas destinadas à proteção de direitos ou de interesses legalmente protegidos de quem invoque o direito a ser indemnizado, sob pena de reconhecer-se – em desvio face à regra geral constante do artigo 483.º, n.º 1, do Código Civil – que a violação de quaisquer normas do RGPD ou de outras que se encontrem previstas em legislação nacional poderem fundar o direito à indemnização, ainda que o lesado não se conte entre aqueles que essas mesmas normas se destinam a proteger.

Neste sentido, a redação do preceito em questão deveria ser mais concretizada, por forma a ir de encontro ao que, em sede geral, se prevê no artigo 483.º, n.º 1, segunda parte, do Código Civil.

A ressalva constante da parte final do artigo 33.º, n.º 2, estabelece uma regra fundamental em matéria de responsabilidade civil e que, de resto, já decorre do artigo 82.º, n.º 3, do RGPD.

Na perspetiva da CIP, o enquadramento estabelecido na PL é o enquadramento geral da responsabilidade civil delitual, pelo que, caso o facto causador do dano não seja

imputável ao responsável ou ao subcontratante, naturalmente que falece qualquer possibilidade de lhes ser assacada responsabilidade civil.

Conclusão diversa caberia se se consagrasse um modelo de responsabilidade civil pelo risco, que prescindisse da culpa do responsável ou do subcontratante, permitindo a imputação de responsabilidade civil a estes últimos caso o facto ilícito tivesse derivado de atos de terceiros a quem lhes incumbisse dirigir ou fiscalizar.

Todavia, tendo em linha de conta que o RGPD não consagra um modelo de responsabilidade civil pelo risco, percebe-se a opção, neste domínio, tomada na PL.

Note-se ainda, a título explicativo, que, nos termos do disposto no artigo 82.º, n.ºs 4 e 5, do RGPD, sendo o facto ilícito imputável a mais do que uma das pessoas referidas no artigo 33.º, n.º 1, qualquer deles é responsável pelo ressarcimento da totalidade dos danos, sem prejuízo de lhe assistir direito de regresso sobre os demais responsáveis.

Esta opção legal traduz, igualmente, uma nota típica da responsabilidade delitual, ao consagrar a regra segundo a qual, em caso de pluralidade de responsáveis, o dever de indemnizar traduz uma responsabilidade solidária, nos termos genericamente consagrados para essa modalidade de responsabilidade civil decorrente do disposto no artigo 497.º, do Código.

30.

A tutela jurisdicional nos termos do artigo 34.º encontra-se demasiado focada nos direitos do titular dos dados, podendo levar à ideia de que o responsável e o subcontratado não têm o direito de impugnar judicialmente qualquer decisão da CNPD.

Mesmo que tal direito se possa inferir da lei geral, seria útil existir clarificação nesse sentido.

Por outro lado, no n.º 2, para efeitos de prova de não imputação de responsabilidade pelo responsável pelo tratamento, pelo subcontratante e pelo encarregado de proteção

de dados, as organizações serão levadas a manter informação, no limite, até à prescrição dessa responsabilidade, cujo prazo ordinário é de 20 anos.

Entendemos que este prazo de conservação, se generalizado, poderá 1) subverter o princípio da limitação da conservação e 2) impor custos acrescidos às organizações, em particular os decorrentes da manutenção de arquivo físico e digital, sendo este último agravado pela obsolescência tecnológica que garantidamente acontecerá num prazo tão alargado.

Assim, sugere-se ao legislador que considere a aplicação de prazos prescricionais mais reduzidos para estes casos.

31.

Relativamente ao artigo 35.º questiona-se se a representação dos titulares dos dados prevista não poderá colidir com o regime da procuradoria ilícita e dos atos próprios dos Advogados, para além de, não sendo sociedades de advogados, não estarem, por conseguinte, obrigadas ao sigilo profissional.

No limite, se a opção legislativa for a de incluir uma exceção ao referido regime dos atos próprios advogados, dever-se-ia regulamentar determinados requisitos funcionais para as referidas associações, nomeadamente a obrigação de serem sempre patrocinadas por advogado em sede jurisdicional e sujeitas ao sigilo profissional no âmbito da sua representação de titulares de dados.

32.

No domínio das contraordenações associadas à proteção de dados pessoais, assiste-se a um alargamento considerável dos tipos contraordenacionais, face ao que se previa na Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais).

Note-se que o RGPD não procedeu à tipificação de quaisquer condutas como contraordenações (o que, a ter sucedido, suscitaria, desde logo, um problema de violação da reserva de Lei imposta pelo artigo 165.º, n.º 1, alínea d), da Constituição da República Portuguesa), tendo, todavia, previsto a graduação das respetivas coimas.

33.

Não obstante a remissão para o regime geral das contraordenações, presumindo-se que se refere ao regime de Decreto-Lei nº 433/82, de 27/10, que aprova o regime do ilícito de mera ordenação social – conhecido como RGCO – dever-se-ia especificar na proposta de regulamentação portuguesa as situações de atenuação especial da coima pois embora prevista a possibilidade no RGCO, a sua concretização depende da referência expressa da possibilidade de atenuação especial na legislação avulsa.

Como sabemos, essa possibilidade permite, nos termos do n.º 3 do artigo 18º do RGCO a redução dos limites máximo e mínimo da coima para metade.

34.

O legislador decidiu criminalizar algumas práticas.

Porém, em Portugal já existe um regime legal ao cibercrime - Lei nº 109/2009 (Lei do Cibercrime) – onde a maioria dos crimes previstos na proposta de lei já estão consagrados.

A fim de evitar entropia teria sido preferível uma remissão para esta lei, sendo que se algum dos crimes não estivesse trabalhado no registo adotado pelo RGPD, as adaptações necessárias e as respetivas alterações seriam inseridas na Lei 109/2009 e não na lei que venha a regulamentar o RGPD.

35.

No elenco de contraordenações muito graves disposto no artigo 37.º, o legislador apenas se refere à não prestação de alguma informação relevante nos termos dos artigo 13.º e 14.º do RGPD como despoletando a responsabilidade contraordenacional dos responsáveis pelo tratamento (artigo 37.ºº nº 1 al. h) da PL), não fazendo qualquer menção da não prestação de informação relativa à identidade do responsável, aos interesses legítimos do responsável, ao prazo de conservação dos dados, à existência de transferências internacionais de dados, entre múltiplos outros aspetos. Esta omissão, a nosso ver, não tem razão de ser, já que não existe fundamento para uma hierarquização

da importância das informações a prestar aos titulares dos dados ao abrigo dos artigos 13.º e 14.º do RGPD.

Por outro lado, a norma do nº 1 alínea b) pode ser interpretada como contrariando o disposto no artigo 6.º do RGPD, ao limitar as bases de licitude ao consentimento ou à lei (importaria também aqui precisar que a base de licitude é o cumprimento de obrigação legal).

O RGPD inclui outras bases de licitude, nomeadamente, as previstas nas al. b), d), e) e f) do n.º 1 do artigo 6.º.

O RGPD não estabelece uma graduação de importância destas bases de licitude, nem permite que o legislador nacional restrinja o respetivo leque. Consequentemente, apenas pode constituir contraordenação a inexistência de base de licitude, independentemente daquela que seja aplicável ao caso concreto.

Por outro lado, sem prejuízo do previsto no RGPD, não podemos deixar de sublinhar a desproporção entre as coimas aplicadas a grandes empresas e às PME's.

36.

No que concerne o artigo 38.º (Contraordenações graves) volta-se a sublinhar, sem prejuízo do previsto no RGPD, a desproporção entre as coimas aplicadas a grandes empresas e às PME's.

36.

A norma prevista na alínea b) do nº 1 do artigo 40º pode ser interpretada como contrariando o disposto no artigo 6.º do RGPD, ao limitar as bases de licitude ao consentimento ou à lei (cumprimento de obrigação legal).

O RGPD inclui outras bases de licitude, nomeadamente, as previstas nas alíneas b), d), e) e f) do n.º 1 do artigo. 6.º.

O RGPD não estabelece uma graduação de importância destas bases de licitude, nem permite que o legislador nacional restrinja o respetivo leque. Consequentemente, apenas pode constituir contraordenação a inexistência de base de licitude, independentemente daquela que seja aplicável ao caso concreto, não se logrando compreender qual o motivo da autonomização do consentimento na formulação da norma.

Por outro lado, a alínea i) do artigo 37.º ao referir "ou dificultar" está a recorrer a um conceito altamente subjetivo.

37.

Na perspetiva da CIP, o artigo 38.º, nº 1, alínea f) deveria clarificar quais as obrigações, cuja violação constitui uma contraordenação.

Se o contrato ou um outro ato normativo celebrado com o subcontratante não mencionar as clausulas correspondentes ao artigo 28º do Regulamento Geral sobre a Proteção de Dados constitui, por si só, uma contraordenação muito grave ?

De acordo com o artigo 28.º, n.º 9, do Regulamento Geral sobre a Proteção de Dados o contrato ou o ato normativo devem ser feitos por escrito.

Na falta, constitui uma contraordenação muito grave ?

A redação do artigo 38.º, nº 1 alínea p) deve ser alterada, passando a ler-se "***p) A restrição das funções do EPD, elencadas no artigo 39º do RGPD;***"

38.

O artigo 39.º elenca três circunstâncias relevantes para a determinação da medida das coimas que não se encontram no RGPD: a situação económica do agente, o carácter continuado da infração e a dimensão da entidade, tendo em conta o número de trabalhadores e a natureza dos serviços prestados.

A relevância da situação económica do agente, enquanto critério para a fixação da coima, decorre atualmente do artigo 18.º, n.º 1, do Regime Geral das Contraordenações

(RGCO), sendo, não obstante, um aspeto controverso, na medida em que o mesmo constitui, em nosso entender, um dado que não deve ser tido em linha de conta para esse efeito.

Na verdade, se se compreende que o benefício económico gerado pela infração assuma relevância para efeitos de fixação do montante da coima, mal se compreende, atendendo à natureza sancionatória do Direito Contraordenacional, que se considere a situação económica da pessoa para tal efeito, já que a mesma não tem, à partida, qualquer ligação com o ilícito, traduzindo apenas a capacidade que a pessoa (singular ou coletiva) tem para pagar a coima.

Sempre poderia argumentar-se que essa consideração teria em vista o ajustamento do valor das coimas nas situações em que a capacidade económica do agente é menor.

Todavia, o que a prática demonstra é uma tendência do recurso a esse critério nas situações em que, tratando-se de pessoas coletivas com um volume de negócios elevado, são impostas coimas coincidentes ou próximas do limite legal máximo, mesmo tratando-se de contraordenações de pouca gravidade.

Não dando o RGPD cobertura a este critério de fixação do valor da coima, talvez se justificasse ponderar a relevância do mesmo, ou mesmo retirar esse critério do artigo 39º.

Por seu turno, no que diz respeito à natureza continuada da infração – que também não constitui critério eleito pelo RGPD para a fixação do montante da coima – importa notar que aquilo que pode estar em causa é apenas a graduação da coima nas situações em que um conjunto de factos típicos é sancionado como uma única contraordenação.

Não está, portanto, tal circunstância relacionada com a reincidência. Neste sentido, a solução avançada na PL vai muito para além daquela que, no regime geral, se encontra prevista no artigo 18.º, n.º 1, do RGCO.

Na PL prevê-se que a culpa releva para efeitos de fixação da coima. Todavia, tendo em linha de conta que a infração continuada consiste numa unidade de ação ocorrida em circunstâncias que determinam a diminuição da culpa do agente, prever que, nesses casos, a coima pode ser superior consubstancia, em nosso entender, uma violação do princípio da culpa, traduzida na valoração mais severa de uma situação em que esta diminui.

Ou seja, na maneira como a norma está formulada na PL, poderá ser determinada uma sanção superior para casos em que a culpa do agente seja menor.

39.

Embora o RGPD refira que a certificação (no âmbito da proteção de dados pessoais) seja voluntária e sabendo que existem atualmente várias normas neste domínio, a alínea s) do artigo 38.º levanta algumas dúvidas quando classifica como "*Infração grave*" (ou seja, que pode ascender a 10 000 000 euros) a "*utilização de selos ou marcas de proteção de dados que não tinham sido emitidos por organismos de certificação devidamente acreditados (...)*".

Esta previsão sugere a possibilidade de alguma falta de isenção e/ou existência de interesses de mercado, podendo dificultar a aplicação de uma solução que nos parece de louvar.

40.

Relativamente ao concurso de infrações e sanções acessórias, a solução vertida nos artigos 55.º e 56 diferem do que atualmente se dispõe no artigo 39.º, da Lei n.º 67/98, de 26 de outubro.

Uma das novidades (mas que está prevista no artigo 20.º, segunda parte, do RGCO), a este propósito, decorre da possibilidade de aplicação das sanções acessórias previstas para as contraordenações, mesmo quando o crime consome a contraordenação, o que implica que possa dar-se a acumulação de sanções acessórias (as que se encontram previstas para os crimes e as que se encontram previstas para as contraordenações),

sendo que, da PL, não consta qualquer norma que estabeleça as condições em que tal possa suceder.

Essa acumulação de sanções acessórias deverá obedecer a critérios de adequação, de proporcionalidade e de razoabilidade que deveriam estar expressamente ressalvados no texto da PL que, neste domínio, transmite a ideia de que é possível a mera acumulação material de sanções acessórias, sem qualquer critério, o que, desde logo, e face ao disposto no artigo 30.º, n.º 4, da Constituição da República Portuguesa, não se nos afigura uma solução adequada.

Por seu turno, no artigo 55.º, n.º 2, prevê-se que, havendo concurso de crime e contraordenação, a competência para o "processamento" da contraordenação cabe às autoridades competentes para o processo criminal.

Esta solução não decorre da Lei n.º 67/98, de 26 de outubro sendo, por isso, inovatória e não corresponde, em nosso entender, à regra de consunção prevista no artigo 20.º, primeira parte, do RGCO.

De facto, parece-nos que o artigo 55.º, n.º 2 deixa em aberto a possibilidade de o agente ter de responder pelo crime e pela contraordenação, uma vez que a consunção está prevista na primeira parte dessa disposição legal mas, a seguir à conjunção "ou" refere-se "quando, pelo mesmo facto, uma pessoa deva responder a título de crime e outra de contraordenação", o que significa que não se trata, aí, de consunção entre responsabilidades, mas de cumulação de responsabilidades.

Esta solução – que é inaudita, em matéria de concurso de ilícito penal e contraordenacional – não obedece à natureza de ultima ratio do Direito Penal, natureza essa que justifica a consunção dos ilícitos contraordenacionais pelos ilícitos penais e justifica-se pela assimetria sancionatória que a Proposta de Lei denuncia (fazendo eco do que se dispõe no RGPD), consistente com a maior severidade das sanções contraordenacionais, em matéria de proteção de dados, face às sanções penais previstas quanto a essa mesma matéria.

41.

No que diz respeito ao destino das coimas, há uma questão que nos parece incontornável e incompreensível: prevê-se, no artigo 42.º que as coimas revertem em 60% do respetivo montante para o Estado e em 40% para a CNPD.

Ora, tendo em conta os poderes da CNPD em termos de fiscalização, correção e sancionamento de situações de eventual incumprimento, mal se compreende que a entidade dotada de tais poderes seja a destinatária de parte do produto das coimas que venham a ser aplicadas no âmbito de processos em que teve intervenção e em que, por determinação legal, tem competência exclusiva para, na fase administrativa, decidir.
Esta solução legal é passível de violar o dever de isenção e de objetividade que norteia a atividade administrativa do Estado, sobretudo quando essa mesma atividade possua um cunho sancionatório.

Esta solução já decorre do artigo 42.º, da Lei n.º 67/98, de 26 de outubro (prevendo-se, aí, todavia, que o montante das coimas reverte, em partes iguais, para o Estado e para a CNPD) mas tal circunstância não retira, em nosso entender, qualquer razão ao apontamento que deixámos feito e que deveria ter sido tido em linha de conta pelo Legislador.

42.

O artigo 44.º (Âmbito de aplicação das contraordenações) refere o seguinte:

"1 - Nos termos do disposto no n.º 7 do artigo 83.º do RGPD, as contraordenações previstas no RGPD e na presente lei não se aplicam às entidades públicas.
2 - Sem prejuízo do disposto no número anterior, as entidades públicas estão sujeitas aos poderes de correção da CNPD previstos no n.º 2 do artigo 58.º do RGPD, com exceção da alínea i), e no n.º 3 do artigo 8.º da presente lei, com exceção da alínea j)."

Neste âmbito, questiona-se: Que razão ou razões justificam, na perspetiva do legislador, a criação de um regime excecional para as entidades públicas ?

É o setor privado, mais uma vez, fonte de todos os males ?

Esta aparente generalização de criar regimes excecionais para o setor público, muito recorrente em projetos de diploma recentemente apresentados, um método de controlo da despesa pública ?

É necessário esclarecer.

Diga-se, desde já, que na perspetiva da CIP, as entidades públicas deveriam estar sujeitas às regras e coimas, à semelhança de qualquer entidade privada.

Por um lado, cabe às entidades públicas dar o exemplo relativamente ao cumprimento das regras relativa à proteção de dados pessoais. Aliás, é essencial para a proteção das pessoas que as entidades públicas, que realizam tratamentos com elevado risco e impacto, fiquem sujeitas a este meio de tutela.

Acresce que, não estando sujeitas a este meio de tutela, deixa de haver um incentivo real ao cumprimento dos princípios e as regras de proteção de dados pessoais.

Além disso, existem situações de coexistência, dentro na mesma organização, de entidades públicas e privadas. Veja-se, a este propósito, os casos de parecerias público privadas no âmbito da gestão hospitalar.

Neste caso, o incumprimento por parte de o hospital não estaria sujeito a contraordenação, ao passo que o mesmo incumprimento cometido pela empresa gestora desse hospital já seria sujeito a contraordenação.

Esta situação de incoerência e insegurança seria incompreensível por parte do cidadão comum.

Por fim, existem situações de concorrência real entre entidades públicas e entidades privadas, sendo certo que a diferenciação a nível da aplicação do regime sancionatório entre as entidades públicas e as privadas introduziria graves desequilíbrios a nível da concorrência que, seguramente, o legislador não pretende promover. Deveria, por isso, o legislador encontrar uma solução a ser plasmada na lei a aprovar, não remetendo para

daqui a 3 anos a apreciação sobre a não aplicabilidade de contraordenações às entidades públicas, como previsto no artigo 59.º da PL.

43.

Os artigos 46.º e seguintes suscitam os seguintes comentários.

A Proposta de Lei prevê novos tipos de legais de crime, nomeadamente a utilização de dados de forma incompatível com a finalidade da recolha, o acesso indevido, o desvio de dados, a viciação ou destruição de dados, a Inserção de dados falsos, a violação do dever de sigilo e a desobediência.

De acordo com a Proposta de Lei, em nenhum destes crimes o procedimento depende de queixa ou de acusação particular.

No entanto, os bens públicos que visam proteger não parecem justificar a qualificação destes crimes como crimes públicos. Aliás, o Código Penal já prevê alguns crimes associados à violação de privacidade, sendo que na maioria dos casos tais crimes são semipúblicos (crf. Artigos 192.º a 195.º do Código Penal).

Ora, a gravidade dos crimes previstos no Código Penal não parece ser inferior à dos novos crimes previstos na Proposta de Lei. Tal como se prevê no Código Penal, a qualificação do crime como público (artigo 193.º) deveria estar reservada para os crimes mais graves e para os casos em que inclui categorias especiais de dados.

44.

O artigo 48.º (Desvio de dados) refere o seguinte:

"1 - Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento, independentemente da finalidade prosseguida, é punido com pena de prisão até um ano ou com pena de multa até 120 dias.

2 - A pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD.

3 - A pena é também agravada para o dobro nos seus limites quando o acesso:
a) For conseguido através de violação de regras técnicas de segurança; ou
b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial."

A previsão contida no n.º 1 suscita junto desta Confederação uma verdadeira perplexidade.

Vejamos.

Em primeiro lugar, não detetamos tal previsão no RGPD.

Em segundo lugar, conceba-se a seguinte situação:

Uma pessoa pede a um amigo uma recomendação e/ou contacto de um qualquer profissional para desempenhar, a titulo de mero exemplo, uma obra em sua casa.

O amigo dá o nome de uma pessoa e o contacto de e-mail, o qual tem a identificação da citada pessoa.

Ora, perante o caso apresentado, questiona-se: Como enquadrar a situação apresentada no artigo em apreço ?

É que, numa interpretação literal do n.º 1, o amigo que forneceu ou cedeu o contacto poderá ser punido com pena de prisão ou multa até 120 dias.

É assim ? É esta a intenção do legislador ?

A aplicação das sanções previstas respeitam os princípios da adequação e proporcionalidade ?

Esta questão tem naturalmente de ser esclarecida e, obrigatoriamente reponderada, se a interpretação literal acima apontada constituir a vontade do legislador.

45.

Relativamente ao artigo 60.º (Situações de tratamentos de dados pessoais pré-existentes), e a manter-se esta dualidade de critérios quanto às notificações e autorizações efetuadas anteriormente à entrada em vigor da lei projetada – não podemos deixar de questionar: as taxas liquidadas pelos pedidos não avaliados pela CNPD [e que caducariam com a entrada em vigor da lei] não deveriam ser devolvidas às entidades que os apresentaram ?

46.

O n.º 1 do artigo 61.º (Renovação do consentimento) prevê o seguinte: *"Quando o tratamento dos dados pessoais em curso à data da entrada em vigor da presente lei se basear no consentimento do respetivo titular, não é necessário obter novo consentimento se o anterior tiver observado as exigências constantes do RGPD."*

O referido número, na prática, tornará inúteis os consentimentos já obtidos (na medida em que não obedeciam ao RGPD) e obrigará a obter novos consentimentos.

Trata-se, na nossa perspetiva, de uma visão extremamente conservadora e garantística do RGPD, indo mesmo contra os pareceres emitidos pelo Grupo de Trabalho da Comissão europeia que elaborou o Regulamento.

É nosso entendimento que esta norma, tal como está, trará prejuízos muito consideráveis à economia como um todo.

Alertamos, também que, não é de nosso conhecimento que outros países europeus tenham adotado norma tão restritiva como esta.

Na prática, esta norma está a tornar ilegais todas as bases de dados existentes no país, mesmo que estas tenham sido obtidas de acordo com as leis vigentes até à entrada em vigor regulamento. Mais grave, a utilização destas bases de dados vai passar a ser punida como crime.

Vejamos um exemplo prático e hipotético de uma empresa que envia uma newsletter a 200 mil pessoas, tendo obtido os contactos dessas pessoas ao longo de 10 anos de atividade, de forma tácita, ou ainda que tenha obtido o consentimento de forma expressa, não tem hoje modo de o comprovar documentalmente. Ora, ambas as formas de captação de dados referidos eram legais de acordo com a lei.

Porém, se a norma em apreço entrar em vigor, então, no caso apontado, ou a empresa contacta essas 200 mil pessoas e obtém o seu consentimento expresso, ou então, não podem enviar mais qualquer comunicação. E, como é natural e óbvio, não se pode ignorar o custo associado a contactar 200 mil pessoas.

Por outro lado, se por exemplo, considerarmos cartões de fidelização, existem muitas empresas portuguesas de pequena e média dimensão com cartões de fidelização, associados à atribuição de descontos e promoções personalizadas, sendo que esta prática constitui uma percentagem razoável do modelo de negócio.

Impor às empresas o garrote de terem que legalizar as bases de dados de acordo com as atuais exigências do RGPD, mesmo quando a obtenção de dados cumpria a anterior norma, é, assim, a nosso ver, a imposição de um custo desproporcional, face às vantagens para os proprietários de dados pessoais unitariamente considerados.

Face ao exposto, sugere-se a seguinte redação:

"*Nos casos em que o tratamento dos dados pessoais em curso à data da entrada em vigor da presente Lei se basear no consentimento do respetivo titular em conformidade com a Lei n.º 67/98 de 26 de outubro, não será necessário obter novo consentimento.*"

47.

O artigo 59.º (Aplicabilidade de coimas às entidades públicas) refere o seguinte: *"A não aplicabilidade de coimas às entidades públicas, prevista no n.º 1 do artigo 44.º da presente lei, deve ser objeto de reavaliação três anos após a entrada em vigor da lei".*

Como a CIP já referiu anteriormente, a norma em apreço merce fortíssimo reparo crítico.

De facto, a não aplicação de coimas às entidades públicas constitui, efetivamente, um fortíssimo incentivo ao relaxe e à descredibilização das entidades públicas.

Por outro lado, as empresas e os cidadãos, nunca verão as entidades públicas serem penalizadas pelas não conformidades, quando geralmente se espera que as entidades publicas sirvam de exemplo ao resto da economia.

Além disso, existem situações de coexistência, dentro na mesma organização, de entidades públicas e privadas.

Veja-se, a este propósito, os casos de parecerias público privadas, no âmbito da gestão hospitalar.

Neste caso, o incumprimento por parte de o hospital não estaria sujeito a contraordenação, ao passo que o mesmo incumprimento cometido pela empresa gestora desse hospital já seria sujeito a contraordenação. Esta situação de incoerência e insegurança seria incompreensível por parte do cidadão comum. Por fim, existem situações de concorrência real entre entidades públicas e entidades privadas. Não seria razoável que umas estivessem sujeitas a um regime sancionatório e outras não.

Por outro lado, é necessário clarificar o sentido e alcance da norma.

Significa que o artigo 59.º deixará de existir uma vez que decorram três anos após a entrada em vigor do diploma ?

Ou que a Assembleia da República fica vinculada a rever a Lei uma vez que decorram esses três anos, debruçando-se sobre a manutenção ou retirada da referida norma do texto da Lei ?

48.

O artigo 64.º (Entrada em vigor) prevê que a *"presente lei entra em vigor no dia seguinte ao da sua publicação."*

A solução proposta é lamentável e manifestamente criticável.

A entrada em vigor no dia seguinte ao da publicação da Lei revela uma total insensibilidade, senão mesmo desrespeito, para com as empresas.

De facto, para além de não relevar a complexidade da matéria, o legislador não concede qualquer margem, em termos temporárias, para a necessária adaptação das empresas.

Diga-se, aliás, que só falta que a CNPD comece a fiscalizar a aplicação da lei dois dias após a entrada em vigor do diploma.

É certo que o RGPD entra em vigor no dia 25 de maio.

Mas também é certo que as empresas não podem ser responsabilizadas pela manifesta inépcia do legislador.

Estamos, assim, mais uma vez, perante um exemplo claro onde o legislador compromete a competitividades das empresas.

- Comentário específico para o setor da saúde

O artigo 20.º limita o direito de acesso aos titulares dos dados nos casos em que exista um "*dever de segredo que seja oponível ao próprio titular dos dados*".

Embora o artigo 3º, nº 3 da Lei de Informação Genética Pessoal e Informação de Saúde (Lei nº 12/2005, de 26 de janeiro) não seja derrogado pela disposição referida, esta parece vir concretizar, em parte, o nº 4 do artigo 15º do RGPD, que dispõe que "*O direito de obter uma cópia* [dos dados pessoais em fase de tratamento] (...) *não prejudica os direitos e as liberdades de terceiros*".

Assim, quando os clientes de um responsável pelo tratamento no setor da saúde solicitem o acesso ao seu processo clínico, o médico responsável pode invocar esta disposição para "*expurgar as suas anotações pessoais e* (...) *não fornecer informações*

sujeitas a segredo de terceiros e não comunicar circunstâncias que, a serem conhecidas pelo paciente, poriam em perigo a sua vida ou seriam suscetíveis de lhe causar grave dano à saúde, física ou psíquica" (artigo. 40º, nº 4 do Regulamento de Deontologia Médica).

- Aspetos omissos

1.

A PL nada refere a propósito do tratamento de dados genéticos.

Porém, considerando a existência da Lei de Informação Genética, importa assegurar que a mesma não restringe ou contraria as definições do RGPD.

2.

No que concerne o Exercício de Direitos do Titular dos Dados, não havendo qualquer referência a propósito da Investigação Científica, importa clarificar que os direitos (todos) são exercidos através do médico investigador, conforme resulta da Lei da Investigação Clínica.

3.

No considerando (13) do Regulamento Geral sobre a Proteção de Dados consta que os Estados Membros são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito da aplicação do presente Regulamento.

Da PL, com exceção da amplitude do montante das coimas, não resulta qualquer especificidade para as empresas de menor dimensão, situação que antecipamos será muito difícil as mesmas.

4.

No considerando (71) do Regulamento Geral sobre a Proteção de Dados relativo ao tratamento automatizado dos dados pessoais, menciona a tomada de decisões com base

desse tratamento, incluindo a definição de perfis deverá ser permitido se expressamente autorizado pelo direito dos Estados Membros aplicável ao responsável.

Não se identifica na PL qualquer menção às autorizações para a tomada de decisões automatizadas.

5.

Existem leis nacionais em vigor que conflituam com as normas do RGPD e que, assim, exigem uma revisão por parte do Legislador nacional.

São exemplos dessas leis a Lei nº 1/2005, de 10 de janeiro (que regula a utilização de câmaras de vídeo), a já referida Lei nº 34/2013, de 16 de maio ("Regime do exercício da atividade de segurança privada"), a Lei das Comunicações Eletrónicas (Lei nº 5/2004, de 10 de fevereiro) e vários diplomas na área da saúde (como o Regulamento Arquivístico dos Hospitais, a Lei de Investigação Clínica ou a Lei de Informação Genética Pessoal e Informação de Saúde).

Não obstante o disposto no artigo 62.º, sugerimos que o Legislador insira uma disposição que esclareça que os tratamentos de dados pessoais cujos pressupostos se baseiem em leis conflituantes com o RGPD permanecem válidos após 25 de maio de 2018, até à efetiva revisão desses diplomas legais.

6.

Adicionalmente, denotamos que a PL faz menção, em vários preceitos, do conceito de "entidade pública".

Já o RGPD se referia a "autoridades e organismos públicos".

Contudo, nenhum dos diplomas define estes conceitos. Isto levanta sérias dificuldades, na medida em que, não existe uma correspondência integral entre a expressão utilizada no RGPD ("autoridades e organismos públicos") e a noção utilizada na Proposta de Lei ("entidades públicas").

Na falta dessa correspondência, poderia defender-se que o critério relevante, para efeitos de aplicação do RGPD, será o da natureza jurídica das entidades. Assim sendo, o Regulamento aplicar-se-á às seguintes pessoas coletivas de direito público:

a. Estado
b. Regiões Autónomas,
c. Autarquias Locais (Municípios e Freguesias)
d. Institutos Públicos
e. Entidades Administrativas Independentes
f. Associações Públicas
g. Entidades Públicas Empresariais (e empresas públicas ? – vd. infra)

A expressão autoridades e organismos públicos pode criar, contudo, algumas dúvidas – com relevantes implicações práticas – quanto ao âmbito de aplicação do Regulamento.

Vejamos o exemplo do Setor Público Empresarial: integram o Setor Público Empresarial as empresas públicas e as entidades públicas empresariais. As *entidades públicas empresariais* são pessoas coletivas de direito público, com natureza empresarial (cf. artigo 56.º do Decreto-Lei n.º 133/2013, de 3 de outubro, que aprova o Regime Jurídico do Setor Empresarial Público) – pelo que a aplicação do Regulamento não suscita dúvidas.

Por sua vez, as *empresas públicas* são organizações empresariais constituídas sob a forma de sociedade de responsabilidade limitada nos termos da lei comercial, nas quais o Estado (ou outras entidades públicas) possam exercer, isolada ou conjuntamente, de forma direta ou indireta, uma influência dominante (cf. artigo 5.º/1 do D.L. n.º 133/2013).

Ora, se se entender que o Regulamento é apenas aplicável às pessoas coletivas de direito público, então não será de aplicar às empresas públicas, criando assim uma assimetria de regimes, dentro do Setor Público Empresarial que, em matéria de proteção de dados, não encontra justificação racional.

Assim, é importante que a Lei de implementação do RGPD venha definir o que se entende por "entidade pública" à luz dessa Lei, de forma a clarificar a que entidades se aplica o regime especial criado pelo projeto de Lei relativo a certos aspetos, tais como a obrigatoriedade de designação de encarregados de proteção de dados na Administração Pública e a isenção do regime contraordenacional.

7.

Existem leis nacionais de implementação do RGPD já adotadas noutros Estados-Membros da UE, que regulam aspetos relevantes e que não se encontram refletidos na Proposta de Lei portuguesa.

Veja-se, por exemplo, as disposições referentes ao DPO previstas na Lei federal de proteção de dados pessoais alemã (Secção 38), onde se prevê a obrigatoriedade da nomeação de um DPO quando o responsável pelo tratamento leve a cabo operações de tratamento de dados sujeitas a uma avaliação de impacto sobre a proteção de dados ("DPIA").

Entendemos que este preceito tem cabimento, atendendo particularmente a uma das funções do DPO: a prestação de aconselhamento no que respeita ao DPIA e ao controlo da sua realização (artigo 39.º nº1 alínea c) do RGPD).

Assim, e refletindo a preocupação do legislador alemão, deixa-se à consideração do Legislador português a previsão de uma disposição semelhante. Sugerimos, para tanto, o aditamento de uma alínea c) ao artigo 18.º com a seguinte redação: "*O tratamento de dados pessoais sujeitos a uma avaliação (obrigatória) de impacto sobre a proteção de dados.*"

Ainda no âmbito das disposições relativas ao DPO, sugerimos a criação de uma disposição (um artigo 9.º-A") que, à semelhança do que sucede na Lei federal alemã (Secção 6), com a epígrafe "Posição do encarregado de proteção de dados", que preveja o seguinte: "*Nas situações de designação obrigatória de encarregado de proteção de dados, quando o responsável pelo tratamento ou o subcontratante tenham designado um trabalhador da empresa como encarregado de proteção, esse trabalhador é*

protegido contra a demissão pelo período de um ano após a data da cessação de funções enquanto encarregado de proteção de dados caso continue a exercer outro tipo de funções na empresa em questão, sem prejuízo das situações em que exista justa causa de despedimento."

8.

Na esteira do plasmado na Lei federal alemã, seria interessante ver previstas, na Lei portuguesa, as situações em que existe um incumprimento de deveres de informação no que respeita ao tratamento de dados para finalidades de avaliação da solvabilidade dos consumidores.

As Secções 30 e 43 da Lei alemã contêm duas disposições particularmente relevantes e que acreditamos que poderiam ser transpostas, ainda que com contornos ligeiramente diferentes, para a Proposta de lei portuguesa: a Secção 30 (1) refere-se ao tratamento de dados para finalidades de avaliação da solvabilidade dos consumidores, prevendo que qualquer organismo que, com o propósito de comunicar esses dados a um terceiro, recolha, armazene ou modifique, com intuito comercial, os dados pessoais que podem ser utilizados para avaliar a solvabilidade dos consumidores, deve tratar os pedidos de informação dos credores em outros Estados-Membros da UE, da mesma forma que trata os pedidos de informações dos credores nacionais.

Por outro lado, a Secção 30 (2) prevê que, nas situações em que uma entidade se recusa a celebrar um contrato de empréstimo ou um contrato relativo a assistência financeira com o consumidor nas informações fornecidas por um organismo referido na subsecção 1, tal entidade deve notificar imediatamente o consumidor dessa recusa e das respetivas informações recebidas nesse contexto.

Tendo em conta o suprarreferido, a Secção 43 (1) da Lei federal alemã prevê que a violação da Secção 30 (1) constitui um delito contraordenacional, na medida em que não se verifica um processamento adequado de um pedido de informação; do mesmo modo, a violação da Secção 30 (2), primeira parte, reveste igualmente a natureza de delito contraordenacional, na medida em que o consumidor não foi informado ou, se o foi, o terá sido de forma incorreta, incompleta ou muito atrasada.

Nos termos da Lei federal alemã, uma infração deste tipo pode ser punida com multa até 50. 000 €.

9.

No mesmo diploma austríaco existe um clausulado relativo ao uso de dados em caso de desastre/catástrofe.

O Parágrafo 48a da Lei de Proteção de Dados Austríaca, prevê a possibilidade da utilização de dados pessoais (inclusivamente categorias especiais de dados) quando esta seja necessária para auxiliar as pessoas diretamente afetadas pelo desastre, de forma a encontrar e identificar pessoas desaparecidas e falecidas e para informar os seus parentes (p. ex., em caso de incêndio num banco, permite-se o tratamento de dados relativos à saúde dos clientes de forma a permitir o seu auxílio).

A este respeito, poderia a Lei portuguesa criar um sistema de compartilhamento de dados pessoais que permita identificar o paradeiro/prestar auxílio aos indivíduos afetados pela catástrofe.

10.

A Proposta não se debruça sobre outras matérias específicas atuais e da maior relevância prática, que deveriam ser cuidadosamente reguladas em cada Estado Membro, tais como a proteção de dados nas decisões individuais automatizadas incluindo a definição de perfis (Profiling), na Cloud (Computação na Nuvem), Big Data e Internet das Coisas (IoT).

11.

De acordo com orientações já emitidas pela Comissão Nacional de Proteção de Dados, o teste de alcoolémia tem de ser executado por um médico do trabalho, por se tratar de dados de saúde.

Sucede que o teste de alcoolémia não é um ato médico, e como tal não tem de ser executado por Médico, de acordo com a opinião da Ordem dos Médicos.

Ora, neste quadro, preconiza-se a manutenção da tendência de a CNPD continuar a agir como até aqui, neste âmbito, continuando a efetuar fiscalizações no pressusposto de que este teste tem que ser feito por médico do trabalho (e instaurando os respetivos processos de contraordenação com a aplicação das consequentes coimas).
Pelo que entendemos que este aspeto deveria ser salvaguardado, incluindo-se na proposta de lei a previsão expressa de que o teste de alcoolémia pode passar a ser feito por qualquer profissional de saúde, técnico de segurança, ou, em caso de inexistência ou impossibilidade dos primeiros, por superior hierárquico do trabalhador.

12.

Apesar de todo este contexto de preocupação com os dados pessoais e com a proteção dos mesmos, o n.º 5 do art.º 32º da Lei 105/2009 continua a prever que o empregador está obrigado a proporcionar a informação constante do Relatório Único (que contém informação sensível) aos trabalhadores da empresa, o que consideramos não fazer sentido nem ser adequado, tanto mais que está expressamente ressalvado que o envio da referida informação às associações patronais e sindicais deve ser expurgado de elementos nominativos (n.º 8 do mesmo artigo).

Pelo que consideramos que a lei deveria alterar o n.º 5 do art.º 32º da Lei 105/2009.

13.

Nos termos do n.º 1 do art.º 17º do Código do Trabalho, o empregador apenas pode solicitar informações relativas à vida privada do trabalhador para avaliar a respetiva aptidão na execução do contrato. Pelo que os dados de condenações penais ficam excluídos, já que não são relevantes para aferir da referida aptidão.

No entanto, a condenação de alguém poderá ser relevante para aferir da idoneidade de um indivíduo para a ocupação de um determinado cargo ao serviço de uma empresa. Por exemplo, parece-nos absolutamente relevante saber se uma pessoa que vai ocupar um cargo de Diretor Financeiro não tem nenhuma condenação por burla ou falsificação de documentos ou abuso de confiança, por hipótese.

Assim, entendemos que a Lei deveria prever a possibilidade de o empregador solicitar aos candidatos a emprego o seu registo criminal.

7.maio.2018

Isabel Cabrita

De:	DAJSL <dajsl@cip.org.pt>
Enviado:	segunda-feira, 7 de maio de 2018 16:16
Para:	Comissão 1ª - CACDLG XIII
Assunto:	Proposta de Lei n.º 120/XIII que assegura a execução, na ordem jurídica interna, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD) - Nota crítica da CIP
Anexos:	PL 120 execução do RGPD - Nota crítica da CIP 7.5.2018.pdf

Exmo. Senhor
Professor Bacelar de Vasconcelos
Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias,

No âmbito das discussões em curso sobre o assunto em epígrafe, junto se envia, em anexo, Nota crítica da CIP sobre a Proposta de Lei n.º 120/XIII que assegura a execução, na ordem jurídica interna, do 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.

Com os melhores cumprimentos.

Luís Henrique

DAJSL - Departamento dos Assuntos Jurídicos e Sócio-Laborais

CIP
CONFEDERAÇÃO EMPRESARIAL DE PORTUGAL

Praça das Indústrias | 1300-307 LISBOA
Tel.: +351 21 316 47 00 | Fax: +351 21 357 99 86
E.mail: **dajsl@cip.org.pt**
www.cip.org.pt