DPO mag

EDIÇÃO Nº 4 · DEZ/21

www.dpo-portugal.pt

APDPO PORTUGAL

www.dpomag.com

DPO mag

EDIÇÃO Nº 4 · DEZ/21

www.dpo-portugal.pt

APDPO PORTUGAL

www.dpomag.com

DPO | magazine

FICHA TÉCNICA

NOME
DPO | magazine

PROPRIEDADE
APDPO Portugal – NIF 541502835

DIRETORA
Inês Oliveira

EDITOR
João Azevedo

PERIODICIDADE
Semestral

PREÇO
Gratuito

CONTACTO GERAL
geral@dpo-portugal.pt

UM PROJETO APDPO
ISSN 2184-8211

Mensagem da Diretora

Inês Oliveira
Presidente da Direção da APDPO
Diretora da DPO Magazine

Bem-vindos ao n.º 4 da DPO Magazine, a revista da APDPO – Associação dos Profissionais de Proteção e de Segurança de Dados!

Neste número trazemos várias novidades, que de seguida passarei a listar. Permitam-me, antes disso, falar-vos das continuidades.

A DPO Magazine continua a ser um projeto de informação da APDPO, que visa contribuir para as áreas de conhecimento atinentes à proteção de dados pessoais, privacidade e segurança da informação. Continua a ser digital e gratuita, independente e livre, sem quaisquer interesses ou hierarquias.

Altos padrões de exigência na qualidade dos artigos continuam a pautar a revista, sendo, pois, a forma de garantir a sua credibilidade.

Continuamos sem fronteiras geográficas, culturais ou temporais, e a recusar situações de sensacionalismo, exploração ou especulação.

A DPO Magazine pretende continuar a fomentar o debate informado e é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e independência.

Vejamos agora as novidades.

A grande novidade é a nova roupagem, a começar pela capa, que passa a ser um traço caracterizador e identitário da revista. Acresce que é intenção da atual direção da APDPO caminhar para uma aproximação às revistas científicas, em que os espaços comerciais e de patrocinadores deixam de ocupar lugar de destaque. Queremos focar-nos sobretudo nos artigos, rigorosos e independentes. Neste n.º 4 encontrarão também duas entrevistas, que permitem aos nossos associados partilharem as suas experiências. Além disso, a DPO Magazine é agora distribuída em pdf, na sequência de

vários pedidos para ser apresentada nessas vestes.

A DPO Magazine, antes bimestral, passa a ser de edição semestral, em junho e dezembro. A redação passou a ser assegurada pela direção da APDPO e a edição por João Azevedo.

Enquanto projeto associativo, encontrarão na DPO Magazine artigos e entrevistas dos associados da APDPO, aos quais aqui deixo um agradecimento público pelo trabalho, entrega e dedicação. Não posso perder a oportunidade, já a pensar na próxima edição, de convidar todos os nossos associados que queiram partilhar conhecimentos e experiências, dando aqui o mote para o próximo número recheado de saberes.

Por agora desejo a todos boas leituras!

Conteúdo

Entrevista a Luís Feliciano, anterior Encarregado da Proteção de Dados da Câmara Municipal de Lisboa

Luís Feliciano
Jurista
Câmara Municipal de Lisboa

Foi um dos protagonistas no escândalo da partilha de dados de manifestantes pelos serviços da Câmara Municipal de Lisboa. Que lições tira relativamente à posição do encarregado da proteção de dados (EPD) dentro de uma organização?

Sim é verdade. Infelizmente, apesar da grande quantidade e complexidade de tratamentos de dados pessoais existentes no Município de Lisboa, ainda que ciente da probabilidade elevada de ocorrência de problemas, sempre encarei a minha missão de Encarregado de Proteção de Dados (EPD) do Município como um desafio e, por tudo quanto foi acontecendo ao longo de pouco mais de três anos de exercício de funções, nada fazia supor que fosse envolvido nesta situação nos termos que são conhecidos e que, quer queiramos quer não, não deixam de deixar marcas do ponto de vista profissional e até mesmo pessoal.

Foi de facto uma situação que poderia ter sido evitada se, atempadamente, ela tivesse chegado ao meu conhecimento como aconteceu com a grande maioria dos tratamentos de dados pessoais realizados no Município, pois permitiria que, além do respetivo registo de atividade, fosse objeto do meu aconselhamento tal como aconteceu em centenas de solicitações dos serviços municipais que me foram dirigidas durante os três anos de exercício de funções.

Mas enfim, o mal está feito como diz o povo e, agora, há que tirar ilações do sucedido.

Uma delas é exatamente o âmago da pergunta que me é dirigida e, seguramente,

a primeira grande lição é de que é muito difícil o posicionamento do EPD num organismo público, não tanto pelas suas funções intrínsecas, pois são similares em qualquer organização pública ou privada, mas sim devido a fatores exógenos como sejam a exposição política inerente a alguns organismos públicos, de que talvez seja um dos maiores expoentes a Câmara Municipal de Lisboa.

Estes fatores exógenos são por natureza incontroláveis e não gostaria de me alongar quanto a eles, mas ainda assim direi que, devido a esta particularidade, mais evidente se torna que será desejável que as funções, os direitos e deveres do EPD e o posicionamento na organização, entre outros aspetos, constem dum documento escrito contratualizado entre as partes, que as obriguem e salvaguardem mutuamente.

Na sua visão, as funções do EPD, mormente a de aconselhamento e a de controlo, estão a ser bem compreendidas pelas chefias?

Só poderei pronunciar-me duma forma mais efetiva relativamente ao contexto que conheço, ou seja, relativamente ao Município de Lisboa.

Aqui, tal como me parece acontecer com a generalidade dos organismos públicos, o RGPD constituiu uma novidade, um novo paradigma, em matérias que sabemos bem já deveriam estar assimiladas pelo menos desde a Lei de Proteção de Dados de 1998 mas, convenhamos, seja por razões culturais, seja porque "é mais fácil" e "sempre se fez assim", subsistem algumas dificuldades de entendimento e aplicação destas "novidades", pelo que, naturalmente, as funções de aconselhamento do EPD sempre foram bem vindas e, posso dizê-lo, sempre senti que são estimadas pela generalidade dos serviços e das chefias.

Já não tão estimadas e bem vindas pelas chefias, são as funções de controlo do EPD, muitas vezes entendidas como intrusão nos procedimentos e competências, o que obriga a um esforço acrescido de desconstrução desta função perante as chefias, no sentido de fazer perceber que acima de tudo estas funções fazem parte das soluções e não dos problemas, que poderão ser assim evitados, mas também para a melhoria da qualidade dos serviços pois, a reboque da atenção para com as questões relativas à proteção de dados pessoais, muito poderão as organizações melhorar em termos de eficácia, eficiência e qualidade dos serviços prestados aos cidadãos.

E não acha que podem ser contraditórias, uma vez que a montante recomenda e a jusante controla muitas vezes o que recomendou?

Sim, de alguma forma podem ser contraditórias. Em especial em organizações de países latinos que, na minha opinião, têm alguma dificuldade em lidar e aceitar a autorresponsabilização e a existência de figuras como o EPD dentro das próprias organizações.

Em países latinos aceitam-se facilmente os Provedores de Justiça, do Ambiente, etc., cujas funções de aconselhamento e contro-

lo, sendo exercidas externamente, quase como entes longínquos, são bem aceites e compreendidas. Já quando estas funções são exercidas dentro das organizações, mesmo por EPD externos, creio que é necessário um estado de maturidade suficientemente robusto no que concerne às temáticas da segurança e da proteção de dados pessoais, em especial nas chefias de topo, o que correntemente não acontece e por isso subsistem dificuldades por vezes inultrapassáveis.

Na minha perspetiva, no elenco de funções cometidas ao EPD no RGPD e na Lei de Execução, podem resumir-se em duas palavras-chave: conselheiro e garante. Ambas caraterizam o essencial das funções do EPD nas várias dimensões da sua atividade, tanto dentro da organização como na relação com os titulares dos dados e com a autoridade de controlo, ambas são as duas faces duma moeda que é a conformidade.

E a conformidade não deixa de ser um caminho que as organizações têm de percorrer, no qual as recomendações têm um papel decisivo, devidamente acompanhadas do controlo que, sendo exercido duma forma proativa e construtiva, não deixa de constituir um prolongamento dessas recomendações e, por vezes, dar origem a novas recomendações.

Penso que é esta a grande missão do EPD. Ajudar as organizações na melhoria contínua também no que se refere à proteção de dados pessoais, aconselhando as melhores práticas nestas matérias, bem como sinalizando as desconformidades na sua função de controlo, o que do meu ponto de vista não é contraditório desde que entendidas no contexto da autorresponsabilização das organizações em que o EPD tem um papel crucial e insubstituível.

Qual o impacto do seu caso em concreto para a figura do EPD?

Penso que será difícil ter-se neste momento uma perceção completa do impacto do sucedido comigo para a figura do EPD.

Em primeira instância, creio que é evidente que o sucedido gerou uma grande preocupação na generalidade dos EPD, o que se compreende, pois, nos termos do RGPD e da Lei de Execução, não é suposto que sejam penalizados ou destituídos pelo exercício das suas funções.

O impacto para os EPD dependerá muito do que as autoridades competentes vierem a decidir no âmbito dos processos em curso, cujas decisões podem ser muito importantes para que a figura do EPD nas organizações possa ser entendida, ouvida e respeitada, oferecendo assim as devidas garantias de independência, essenciais para a confiança dos titulares dos dados que interagem com essas organizações e da sociedade em geral.

Uma coisa posso dizer e com isso termino: quando fui convidado a demitir-me, recusei de imediato ainda que ciente de que esta minha decisão poderia complicar tanto a minha situação como a do decisor mas, em consciência, o que verbalizei em resposta, não poderia aceitar demitir-me eu próprio pela certeza do bom trabalho desenvolvido, reconhecido tanto interna como exter-

namente em vários momentos, pelo respeito que me merecia a equipa reduzida que me acompanhava e as quase duas centenas de trabalhadores que, nos seus serviços, desempenhavam funções de interlocução em matéria de proteção de dados pessoais e, não menos importante, pelo facto dessa minha eventual decisão vir a gerar uma grande preocupação nos colegas EPD, pois constituiria um precedente que, a fazer escola, colocava em causa a posição dos EPD nas organizações, bem como, a concretizar-se ao arrepio do que estabelece o RGPD, comprometeria de alguma forma a missão de todos os EPD do nosso país.

O desenlace é de todos conhecido e, como já tive oportunidade de transmitir em várias instâncias, temos a capacidade de aprender com as coisas boas e as menos boas. Pelo que, quanto mais não seja, este episódio poderá contribuir para uma reflexão mais profunda dentro das organizações no que respeita aos tratamentos de dados pessoais que realizam, bem como para enquadrarem melhor os respetivos EPD, envolvendo-os devidamente tal como estabelece o RGPD.

A vida continua e, apesar da nossa função como EPD ser uma novidade e ter algumas dores de crescimento no modo como as organizações o entendem, aceitam e apoiam, estou confiante de que, apesar de difícil, acredito que a breve trecho será inevitável o reconhecimento e a tomada de consciência da importância dos EPD para as organizações e para a defesa dos direitos dos titulares dos dados, os quais são, em última instância e em boa verdade, a razão de ser da nossa existência.

O RGPD na Administração Pública
O Paradigma do Município de Lisboa

Pedro João de Oliveira
Encarregado de Dados Pessoais
Município de Salvaterra de Magos

O Regulamento Geral sobre a Proteção de Dados (RGPD), em aplicação desde 25 de maio de 2018, não distingue (na previsão nem na sua aplicação) administração pública de setor empresarial privado.

Tal como não há distinção patente na legislação ordinária nacional, entretanto publicada, pelas Leis n.º 58/2019 (execução do regulamento – RGPD - no ordenamento jurídico nacional) e 59/2019 (aprovação das regras relativas ao tratamento de dados pessoais para fins penais), ambas de 8 de agosto de 2019.

Tratar a proteção de dados pessoais de igual forma não é critério e demonstra negligência por parte das autoridades com competência na matéria, as quais não cuidaram de adaptar a diversa legislação existente ao regulamento comunitário, salvo raras exceções, como demonstra a Lei de Acesso aos Documentos Administrativos (LADA), aprovada pela Lei n.º 26/2016.

Ora, se por um lado o consentimento do titular dos dados é regra no setor empresarial de índole privada, aquele é meramente supletivo na parte da administração pública.

Isto porque a administração pública não tem qualquer interesse na captação de dados, apenas necessita daqueles para prosseguir os seus fins e atribuições, os quais no interesse do cidadão (titular dos dados).

Já o setor empresarial de índole privada, tem interesse nos dados pessoais para transacionar (entre empresas) ou elaborar (para si) perfis tendo por intuito a transação comercial.

Importava acautelar os interesses dos cidadãos face à massificação de dados transacionados ou simplesmente compilados pelas empresas tecnológicas de refe-

rência, quando tais dados pessoais eram (e continuam a ser) voluntariamente cedidos pelos próprios.

A aplicação do RGPD à administração pública é de cariz diametralmente oposto aquele que se pretende no setor empresarial privado, não sendo, ainda assim, despiciendo, não tutela a elaboração de perfis ou transação de dados para fins comerciais.

Isto porque a administração pública não faz transações comerciais, atua no âmbito do princípio da legalidade, fazendo uso dos dados para fins específicos, os quais devidamente consagrados no RGPD, como execução de contrato, cumprimento de obrigação jurídica, para a defesa de interesses vitais ou para o efeito da prossecução de interesses públicos, tornando o consentimento meramente supletivo e para casos muito excecionais.

No entanto, o RGPD é muito importante para a administração pública, pois veio permitir a análise dos procedimentos tendentes ao ato administrativo, a sua adequação e modernização, tal como a aposta na segurança informática.

Uma administração pública que se tornou pelo menos no meio autárquico mais leve e mais preocupada com o uso dos dados pessoais, no tratamento dos processos administrativos, bem como na sua difusão / permissão de consulta ou reprodução de documentos, expurgando e eliminando práticas "milenares" sem qualquer aplicação plausível, como o pedido de todos os dados pessoais e mais alguns.

Procedeu-se em geral, à adequação de formulários, reorganização de procedimentos, aposta na segurança informática e na disponibilização de informação acerca dos direitos dos titulares.

E o que se passou no Município de Lisboa?

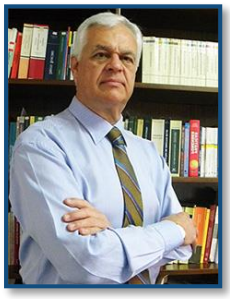
Uma violação grosseira do princípio da legalidade a que aquele município (como os restantes) se encontra adstrito.

A questão da partilha dos dados pessoais de todos os manifestantes pelo município de Lisboa com terceiros (os visados pelas manifestações) é muito mais profunda que a violação do RGPD, trata-se de um procedimento administrativo sem motivação de suporte e por consequência ilícito.

Tal prática (pelo Município de Lisboa) é anterior ao RGPD e nem por isso legitimo, nem legitimado (ou enquadrável) pela Lei, invocada pelos responsáveis daquele Município.

A administração pública pode e deve aproveitar a oportunidade de adequar os seus procedimentos ao RGPD, modernizando-se, tornando-se mais ágil e segura, abolindo os pedidos e trâmites desnecessários, tendentes ao ato administrativo mais célere, transparente e profícuo.

III Encontro Nacional da APDPO
Dois passos em frente!



Sílvio Gomes
Sócio e gerente / Direcção de Projectos
Compliance Way

No passado dia 23 de Novembro, a APDPO realizou o III Encontro Nacional. Participantes interessados e convidados excelentes, debateram temas pertinentes.

Depois de sofrer um pequeno sobressalto, que pode considerar-se de definição e crescimento, organizou o seu primeiro evento com visibilidade e manifesto interesse público, na prossecução do seu propósito associativo, focado no papel do DPO, acrónimo anglicista de encarregado da protecção de dados.

Cumpriram-se as expectativas quanto à necessidade e à oportunidade do evento, em especial no actual quadro político instável e incerto, cujo desfecho não será indiferente ao ritmo e ao sentido do desenvolvimento dos temas da protecção de dados pessoais.

Um abalo e dois passos à frente

Para além da qualidade do evento, sentiu-se que algo conferiu ao Encontro um "gostinho especial", uma vez que, só formalmente, veio na sequência natural dos encontros anteriores.

Durante a viagem entre o II e o III Encontro verificou-se um percalço associativo, cujo impacto negativo na imagem da associação e nas convicções de alguns, tiveram as suas consequências controladas e recuperáveis.

Alguns temas menores, ainda que com a sua relevância, foram trazidos a debate de modo desbragado, e sem um enquadramento programático, quanto aos caminhos a seguir - que fazer e por onde ir?

Ultrapassado o frenesim para utilizar a associação na alavancagem de um modelo

de negócio, tenha lá os êxitos que tiver, sentiu-se o gostinho dos novos desafios que se colocam, existam as dificuldades que existirem.

O caminho que vem sendo consistentemente seguido pela APDPO, de promover reflexões sobre si mesma, para melhor olhar para fora, dá uma nova confiança.

De facto, só um corpo de ideias, princípios e regras claras, formado em debates, tão serenos quanto profundos, pode responder às necessidades e expectativas dos DPOs, ambicionando constituir-se como a sua força associativa.

Ao ganhar mais escala, a APDPO ganhará mais voz e poderá ter uma maior capacidade de influenciar e contribuir para um desenvolvimento económico e social, no respeito pela protecção das pessoas singulares, quanto aos seus dados pessoais, como um direito fundamental.

Nem reconhecida, nem regulada

Não é fácil o exercício da função de DPO, ainda sem o reconhecimento de categoria profissional e sem regulação específica, num ambiente de cultura organizacional em que a protecção de dados está ausente.

Entre gestores, administrativos, técnicos, comerciais e outras categorias profissionais, vistas pela "Alta Direcção" como integrantes da cadeia de valor, surge o DPO, actor surpresa de um tema exotérico e pouco atraente para as organizações que têm que os designar.

Excepções à parte, são raras as organizações que olham para o gasto com o DPO, como uma oportunidade para reorganizarem os serviços e acertarem o passo dos fluxos das actividades, pela conformidade legal aplicável à protecção de dados.

A maioria das organizações preocupa-se mais em criar barreiras dinâmicas de opacidade variável, e em jogar às escondidas com o DPO.

A natureza descritiva da maioria das organizações, avessa aos "empecilhos" da normalização e da regulamentação, mantém a inércia da gestão procedimental e das práticas cristalizadas ao longo dos anos.

Ao arrepio da conformidade legal

Por múltiplas razões, e normalmente sem razão, as entidades públicas e privadas, em especial grandes empresas ou grupos empresariais, seguem os velhos hábitos de tratar os dados pessoais como uma mercadoria oferecida, e em mercado livre.

Acusam o incómodo de serem obrigadas a admitir que os dados são dos titulares e têm de ser tratados para finalidades específicas, com transparência e licitude, entre outros princípios a observar.

Em muitas empresas, em especial PME do tecido empresarial tradicional, a baixa literacia e cultura de liderança e gestão, a procura simplista da agilidade operacional sem atender à segurança da informação e do tratamento de dados, bem como algumas dificuldades de recursos, não são estranhos ao estado de desadequação face ao RGPD e à Lei 58/2019 (Lei).

Outras existem que, sendo PME do tecido empresarial mais moderno, ou grandes

empresas e grupos empresariais, se arrogam no direito de driblar a regulamentação da protecção de dados e decidir apenas de acordo com os seus interesses de negócio, atropelando "silenciosamente" os direitos dos titulares.

Esta desadequação é estudada e avaliada face à significância do risco sancionatório que comporta, no ambiente "virtual" do poder fiscalizador da autoridade de controlo, que continua sem que lhe sejam proporcionados os recursos e as condições para uma actuação efectiva e adequada, própria de uma autoridade administrativa independente, com um mandato constitucional previsto no Direito Europeu.

O texto e o contexto

Existem tensões conflituantes entre os requisitos e critérios estabelecidos no texto, leia-se o RGPD e a Lei, e o contexto, leia-se cada organização.

Pelo que vou conhecendo e vivendo, os DPOs vivem um contexto ao arrepio do texto.

Quando avançam com o registo das actividades de tratamento, orgulhosos e decididos, sob a autoridade e o poder consultivo conferido pelos artigos 37.º a 39.º do RGPD, para verificarem se não estão a ocorrer operações de tratamento "estranhas", depressa sentem uma mão (in)visível a sair da opacidade e a colocar novas barreiras.

Admito que existam saudáveis excepções, mas que a maioria das organizações não está a acomodar a ideia de terem de conviver com um "Príncipe Perfeito", a pairar sobre as operações de tratamento diárias, e que, do alto da sua gávea, quer saber e meter-se "em tudo", parece uma evidência.

Encaremo-la de frente, e numa gestão do risco associado ao seu exercício, poderemos traçar um quadro razoavelmente objectivo e contribuir para se ultrapassar o estado alquimista do nosso "esboço de profissão".

Acredito que o novo fôlego da APDPO, ao dar dois passos em frente no modelo associativo focado no papel do DPO, permitirá realizar o seu propósito.

As sanções administrativas no quadro do tratamento de dados pessoais relacionados com condenações penais e infrações

Augusto Cesar Torbay
DPO/Jurista
Autoridade Nacional de Segurança Rodoviária (ANSR)

Enquanto profissionais da proteção de dados pessoais, diariamente somos confrontados com as consequências das opções linguísticas do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados, doravante RGPD). Desde logo, a mais gritante é a circunstância de termos de denominar como "*subcontratante*" uma entidade "*contratada*", algo que nos exige a todos, sempre, algum esclarecimento.

Embora em certos casos baste uma breve nota para esclarecer pequenas incorreções técnicas, existem outras instâncias que demandam algum esforço hermenêutico na sua concretização.

Uma manifestação desta realidade é o regime consagrado pelo RGPD ao tratamento de dados pessoais relacionados com condenações penais e infrações. Na sua versão portuguesa, o art.º 10.º do RGPD, tanto no seu corpo como na respetiva epígrafe, vem subsumir a sua aplicação ao "(…) *tratamento de dados pessoais relacionados com* ***condenações penais e infrações***"[1] (negrito nosso).

[1] Aliás, sempre que este Regulamento remete para o regime do art.º 10.º, a remissão é realizada através da referência a "*condenações penais e infrações*" (é o que sucede na al. c) do n.º 4 do art.º 6.º, na al. a) do n.º 2 do art.º 27.º, no n.º 5 do art.º 30.º, na al. b) do n.º 3 do art.º 35.º, na al. c) do n.º 1 do art.º 37.º e, ainda, nos considerandos 75, 80, 91 e 97.

Observando que é concedido um regime particularmente reforçado de tutela a estes dados pessoais (designadamente, nos termos da al. b) do n.º 3 do art.º 35.º do RGPD), caberá ponderar a efetiva extensão do respetivo âmbito de aplicação.

Uma interpretação literal da norma parece sugerir que esta se subsume a todo o género de infrações (entenda-se, tanto "*penais*" como "*administrativas*"). Desde logo, o posicionamento do adjetivo "*penais*", imediatamente após o termo "*condenações*", cria a impressão de que o legislador procurou incluir no escopo da norma a generalidade das "*infrações*", ou seja, tanto as de caráter penal, como as de natureza administrativa (diversamente do que ocorreria se a norma referisse "condenações e infrações **penais**" em lugar de "*condenações **penais** e infrações"*).

Sucede, porém, que tal entendimento é patentemente incongruente com o elemento histórico da norma. Por um lado, o legislador da União ativamente rejeitou a inclusão do termo "*sanções administrativas*" (sugerida pelo Parlamento Europeu[2]) aquando da redação do artigo. Por outro lado, é um facto que o art.º 10.º do RGPD veio suceder ao n.º 5 do art.º 8.º da Diretiva 95/46/CE de 24 de outubro de 1995, o qual se destinava, exclusivamente, a regular o "*tratamento de dados relativos a **infrações, condenações penais ou medidas de segurança***" (negrito nosso), deixando de fora as "*sanções administrativas*" (cuja inclusão era deixada à disposição dos Estados-Membros).

Esta perspetiva obriga-nos a considerar que o legislador da União não pretendeu o alargamento, *qua tale*, do âmbito de aplicação do art.º 10.º do RGPD à generalidade de infrações administrativas. Consequentemente, entendemos que este artigo deverá ser objeto de uma interpretação restritiva que, muito embora venha embater frontalmente com a respetiva letra, tem o condão de suprir a incongruência da sua interpretação literal.

Do nosso ponto de vista, a inconsistência resultante do seu elemento literal poderá derivar de um lapso de tradução, o qual se torna exponencialmente evidente à medida que a comparamos com outras versões linguísticas.

Como ponto de partida, podemos comparar com a versão espanhola, devido à sua proximidade com o português a nível de sintaxe. Nos termos da sua redação, a referência a "*condenações penais e infrações*" é substituída por "*condenações e infrações penais*" ("*condenas e infracciones penales*"). Ou seja, na versão castelhana, torna-se evidente que a referência a "*penais*" ("*penales*") destina-se tanto às "*condenações*" ("*condenas*") como às "*infrações*" ("*infracciones*").

Esta leitura, parece-nos, salvo melhor opinião, inteiramente mais coerente com o contexto que enquadrou a respetiva redação.

Aliás, se procurarmos o mote que poderá ter fomentado a atual formulação da versão portuguesa, poderíamos ser levados a su-

[2] À data ainda enquadrada no âmbito do art.º 9.º do RGPD, ponderou-se que a norma visasse, expressamente, "*sanções administrativas, julgamentos, delitos penais, condenações (…) ou outras medidas de segurança conexas*" (JO 2017, C378, p.430).

por que se trata de uma tradução literal da versão inglesa, a qual, pela sintaxe que lhe é própria, refere "*criminal convictions and offences*".

Nesta medida, entendemos que a tradução correta para a língua portuguesa, à semelhança do que acontece com a língua castelhana, seria "*condenações e infrações penais*".

Foi precisamente neste sentido que se pronunciou o Advogado-Geral Maciej Szpunar, nas suas conclusões de 17 de dezembro de 2020, no âmbito do processo C-439/19, EU:C:2020:1054, referindo que "*[a] este respeito, algumas versões linguísticas não deixam margem para dúvidas: as «infrações» na aceção do artigo 10.° do RGPD devem ser entendidas no sentido de «infrações penais»*". Conclui, assim, o referido Advogado-Geral, que "*com base numa leitura comparada das diferentes versões linguísticas do artigo 10.° do RGPD, o termo «penal» se refere tanto às «condenações» como às «infrações»*".

Por outro lado, o Acórdão[3] subsequentemente proferido no âmbito do mesmo processo (embora tenha acabado por decidir em sentido diverso quanto à questão material), foi perentório em entender que "(…) *o legislador da União, ao não incluir deliberadamente o adjetivo «administrativo» no artigo 10.º do RGPD,* ***pretendeu reservar a proteção acrescida prevista nesta disposição apenas ao domínio penal***" (negrito nosso).

Alicerçados nestas considerações, entendemos que o art.º 10.º do RGPD deverá ser objeto de uma interpretação restritiva, englobando no seu âmbito apenas infrações e condenações de natureza penal. Mais, pugnamos – conforme já o fizemos em sede própria –, pela correção da tradução ora em causa, substituindo-se a referência a "*condenações penais e infrações*" por "*condenações e infrações penais*" (não apenas no contexto do art.º 10.º, mas na generalidade das remissões ao respetivo regime).

Contudo, e conforme decorre dos fundamentos da citada jurisprudência, devemos atender ao facto de que esta interpretação não impede que uma determinada infração (embora não qualificada como "penal" à luz do direito de um determinado Estado-Membro) seja suscetível de revestir "*caráter penal*" – em decorrência da respetiva natureza e do seu regime sancionatório[4] –, e que, em resultado de tal conjetura, possa recair no âmbito de aplicação desta norma.

[3] Acórdão do Tribunal de Justiça de 22 de junho de 2021, C-439/19, EU:C:2021:504, n.º 78.

[4] Acórdão do Tribunal de Justiça de 22 de junho de 2021, C-439/19, EU:C:2021:504, n.º 88.

EPD, Notificações, Análises de Privacidade e o Decreto-Lei n.º 65/2021

Pedro Santos
EPD / Consultor
Município de Portimão
Revela Regras, Lda

Foi publicado em Diário da República, a 30 de julho de 2021, o Decreto-Lei n.º 65/2021, que regulamenta o Regime Jurídico da Segurança do Ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

O Decreto-Lei n.º 65/2021, que entrou em vigor no dia 9 de agosto, no seu articulado, introduz uma série de novas obrigações a algumas entidades, onde se destacam todos os Organismos da Administração Pública, com obrigatoriedades de reporte ao Centro Nacional de Cibersegurança (CNCS), à semelhança do que acontece atualmente com algumas obrigatoriedades de reporte no que à proteção de dados diz respeito, dirigidos à Comissão Nacional de Proteção de Dados (CNPD).

Neste artigo vamos tentar demonstrar a importância da necessidade de conjugação das responsabilidades e dos deveres previstos na citada legislação com o previsto no Regulamento Geral sobre a Proteção de Dados (RGPD), sendo intenção mostrar as diferenças entre os regimes aplicáveis, incluindo as incompatibilidades e conflitos de interesse inerentes à acumulação das funções de responsável pela segurança e encarregado de proteção de dados (EPD).

Notificação de violação de dados e a notificação de incidentes de segurança

No artigo 33.º do RGPD, epigrafado de "Notificação de uma violação de dados pes-

soais à autoridade de controlo", existe o dever de cada responsável pelo tratamento de dados de notificar a Autoridade de Controlo competente sempre que haja a ocorrência de violação de dados pessoais com risco para os direitos e liberdades das pessoas singulares. No n.º 2 do mesmo artigo está prevista, por sua vez, a obrigatoriedade do subcontratante notificar o responsável pelo tratamento, o que deve ficar plasmado no contrato de prestação de serviços ou em adenda ao mesmo.

No n.º 3 do artigo 33.º do RGPD é indicado o conteúdo mínimo a constar da comunicação, e que deve incluir a descrição da natureza da violação, número de titulares afetados, categoria de registos de dados pessoais em causa e categorias de titulares. Existindo EPD nomeado, deverão ser comunicados os contatos do mesmo, ou não existindo EDP, deverá ser comunicado um outro ponto de contato onde possam ser obtidas mais informações. Deverá ser ainda feita uma descrição das prováveis consequências da violação de dados, assim como quais as medidas adotadas ou propostas adotar para reparar a violação, e se caso disso, medidas tomadas ou necessárias para atenuar eventuais efeitos negativos.

Na Lei n.º 46/2018, o artigo 15.º estabelece a obrigatoriedade de notificação de incidentes com um impacto relevante na segurança das redes e dos sistemas de informação. Já o n.º 4 do citado artigo estabelece os parâmetros da comunicação, mas é depois o Decreto-Lei n.º 65/2021 que melhor definirá os requisitos e necessidades destas notificações. No artigo 19.º da Lei n.º 46/2018 é imposto também o dever de notificação e no n.º 4 do mesmo artigo a indicação dos parâmetros a conter na notificação.

No que diz respeito ao Decreto-Lei n.º 65/2021, é no Capítulo IV, artigo 11.º e seguintes, que está regulada a obrigação de notificação de incidentes. Vejamos o n.º 1 do artigo 11.º: "A Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais notificam o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço.". Ao invés do que acontece com a legislação referente à proteção dos dados pessoais, esta, no artigo 16.º, criou uma taxonomia de incidentes e de efeitos onde é dada importância à causa do incidente e ao efeito, onde, apesar de não vir listado no n.º 2 do mesmo artigo, um dos efeitos poderá ser exatamente o comprometimento de dados pessoais sob a responsabilidade da Entidade afetada.

Importa perceber aqui o conceito constante do n.º 12 do artigo 4º do RGPD: "«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento [sublinhado nosso]. Definição esta que nos leva à alínea c) do artigo 3.º da Lei n.º 46/2018: "«Incidente», um evento com um efeito adverso real na segurança

das redes e dos sistemas de informação;" [sublinhado nosso]. Podemos concluir que uma violação de dados pessoais é um incidente real que de alguma forma provocou um tratamento acidental ou ilícito de dados pessoais com possível impacto negativo nos seus titulares.

Nem todos os incidentes a notificar ao CNCS terão um cariz de risco para dados pessoais, no entanto esta avaliação deverá ser sempre efetuada, por forma a perceber se no decorrer de um incidente de segurança não estarão em causa tratamentos ilícitos de dados pessoais e que devam ser também comunicados à CNPD, em termos distintos e conforme legislação já apresentada.

Nas questões de violações de segurança, a divulgação de dados pessoais de forma acidental, ou por desconhecimento ou inexistência de procedimento correto para o tratamento, deverá ser considerado um incidente de segurança, onde o recurso humano com falta de formação se torna, mesmo que inconscientemente, a origem da violação dos dados. Se este tipo de atos não colocar em causa a segurança das redes e dos sistemas de informação, não haverá necessidade de notificação ao CNCS, mas apenas à CNPD, se em causa estiverem riscos para as pessoas singulares.

Avaliações de Impacto e Análises de Risco

Com a entrada em vigor do RGPD, e com o novo paradigma assente na análise do risco a cargo das organizações, o artigo 35.º impõe a necessidade da elaboração de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), desde logo sempre que este seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas. No entanto, além do previsto no n.º 1 do artigo 35.º, o Regulamento n.º 1/2018 da CNPD relativo à lista de tratamentos de dados pessoais sujeitos a AIPD elenca a obrigatoriedade de elaboração da AIPD em nove tipos de tratamentos neste identificados.

A AIPD deve incluir toda a informação relevante sobre o tratamento, e pelo menos as determinadas no n.º 7 do artigo 35.º do RGPD, que, nas suas alíneas c) e d), preveem "Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1;" e "As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa." [sublinhado nosso].

Importante referir que as AIPD não são da responsabilidade do Encarregado da Proteção de Dados (EPD), devendo, no entanto, ser-lhe solicitado parecer e orientações sobre as mesmas (cf. artigo 35.º n.º 2 alínea c) e artigo 39.º n.º 1 do RGPD).

Na Lei n.º 46/2018, no artigo 14.º, é determinado que quer a Administração Pública quer os operadores de infraestruturas críticas devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segu-

rança das redes e sistemas de informação, garantindo que na ocorrência de incidentes o seu impacto seja reduzido ao mínimo. Em relação aos prestadores de serviços digitais, no artigo 18.º da Lei n.º 46/2018 é imposto as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos.

No Decreto-Lei n.º 65/2021, no Capítulo III, é consagrado o dever de elaborar análises de risco relativas aos ativos que garantam a continuidade. Estas análises deverão ser anuais, após notificação de um risco por parte do CNCS ou sempre que haja alterações ou ocorrências nos sistemas que possam inserir ou alterar os riscos associados.

De notar que as análises de risco diferem das AIPD no que se refere ao alvo ou foco em análise, sendo que numa análise de risco o foco é a instituição e o valor dos seus ativos relativamente às ameaças e vulnerabilidades identificadas, pelo contrário numa AIPD o foco é o titular dos dados no que se refere às suas liberdades e garantias. Deixar, no entanto, a importante nota que não é possível efetuar uma AIPD sem conhecer os riscos associados aos ativos inerentes no tratamento dos dados pessoais, pelo que indiretamente as análises de risco já seriam obrigatórias por questões de segurança na legislação da proteção de dados.

O Encarregado da Proteção de Dados e o Responsável da Segurança

Prescreve o artigo 37.º n.º 1 do RGPD que "O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados…", sendo a sua obrigatoriedade aplicada a toda a Administração Pública e Autoridades, excetuando tribunais no exercício da sua função jurisdicional (cf. alínea a) do n.º 1 do artigo 37.º do RGPD e artigo 12.º da Lei n.º 58/2019). Em relação aos privados, a nomeação pode ser opcional para os que assim acharem conveniente, ou obrigatória mediante a análise de alguns requisitos (cf. alíneas b) e c) do n.º 1 do artigo 37.º do RGPD e artigo 13.º da Lei n.º 58/2019). Esta designação deve ser comunicada à autoridade de controlo, em Portugal à CNPD (n.º 7 do artigo 37.º do RGPD).

Cabe no âmbito do Decreto-Lei n.º 65/2021, no artigo 4.º, a indicação de, pelo menos, um ponto de contato permanente com o CNCS para a garantia dos fluxos de informação a nível operacional e técnico. No artigo 5.º vem a exigência de designação de um responsável de segurança, com a responsabilidade de gestão das medidas adotadas em matéria de requisitos de segurança. Esta obrigatoriedade engloba toda a Administração Pública, operadores de serviços essenciais, infraestruturas críticas e prestadores de serviços digitais (n.º 1 do artigo 2.º da Lei n.º 46/2018, conjugado com o n.º 1 do artigo 2.º do Decreto-Lei n.º 65/2021). Estas designações devem ser comunicadas ao CNCS, nos termos do n.º 3 do artigo 4.º e do n.º 2 do artigo 5.º do Decreto-Lei n.º 65/2021.

Haverá porventura a tentação de confundir estas funções como podendo ser as mesmas, ou até podendo ser efetivadas pela mesma pessoa. Independentemente

das capacidades técnicas e conhecimentos que possam existir para o exercício das funções, o EPD não poderá desempenhar as funções de Responsável da Segurança por conflito de interesses. O Responsável da Segurança deverá determinar os meios e formas no garante da segurança, procedimentos, políticas, controlos aplicados, que o EPD estará impossibilitado de o fazer. Caberá ao EPD poder avaliar as opções e emitir parecer ou orientações no que à segurança dos dados pessoais, direitos e liberdades das pessoas singulares diz respeito, ajudando assim na melhor definição dos meios. O EPD deverá ser visto como um garante da proteção de dados em cada instituição, e não poderá ser responsável na aplicação e efetivação de tratamentos ou meios de tratamento. Se o for haverá conflito de interesses (cf. n.º 6 do artigo 38º do RGPD Orientações do WP29 sobre os encarregados da proteção de dados (WP243rev1)).

Conclusão e Opinião

Não é possível garantir o direito à privacidade e proteção dos dados pessoais sem aplicar todas as medidas técnicas e organizativas (n.º 1 do artigo 24º do RGPD), no que respeita à segurança da informação, até porque dados pessoais são uma categoria especial de informação que deverá ser protegida mediante os riscos apresentados (cf. n.º 1 e n.º 2 do artigo 32º do RGPD e considerados 83, 74, 75, 76 e 77).

No que respeita à Segurança da Informação, Confidencialidade, Integridade e Disponibilidade, não é possível sem a devida segurança das redes e sistemas onde esta informação é tratada, transmitida, armazenada, e diria que até mesmo eliminada pois este tratamento não deixa de ser tanto ou mais importante que os outros, e convém ser efetivado com a maior das garantias de eficácia e segurança. A base da garantia da informação e proteção de dados é a efetivação real de análises de risco que permitam aferir mediante o valor dos ativos, vulnerabilidades conhecidas e possíveis ameaças, todas as medidas necessárias para eliminar, mitigar ou até quem sabe transferir os riscos. No tratamento correto do risco, estar-se-á a responder à parte técnica da AIPD no garante dos direitos das pessoas singulares, mas uma análise de risco não é uma AIPD, sendo só uma parte da mesma.

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

CNCS Centro Nacional de Cibersegurança PORTUGAL

CNPD Comissão Nacional de Proteção de Dados

Apesar de, para muitos, o EPD parecer ser responsável pela segurança, será preciso entender que a sua responsabilidade só está no dever de orientar o responsável pelo tratamento sobre a necessidade de aplicar medidas técnicas e organizativas na segurança dos dados pessoais, mas nunca na

determinação das mesmas, até porque a determinação de controlos na sua grande maioria implica determinar tratamento de dados pessoais, que cabe ao EPD monitorizar a conformidade.

Assim conclui-se que o Decreto-Lei n.º 65/2021 vem ajudar no trabalho necessário à garantia da informação e proteção de dados pessoais, obrigando pelo menos nas organizações dentro do seu âmbito de aplicação à aplicação direta de medidas de segurança que por sua vez melhoram o trabalho necessário na conformidade com o RGPD, não devendo no entanto ser visto como um complemento à legislação existente sobre proteção de dados nem como mais obrigações para o EPD.

É de interesse também referir que em termos de legislação sobre a matéria de segurança de redes e serviços de informação, já tínhamos visto na Lei das Comunicações Eletrónicas, Lei n.º 5/2004 na sua versão atual, igual preocupação no que respeita aos serviços de comunicações eletrónicas e seus prestadores, nomeadamente no artigo 54.º-A "Obrigações das empresas em matéria de segurança e integridade" e artigo 54º-B "Obrigações de Notificação". No artigo 54.º-C "Medidas de execução", é deixada à Autoridade Reguladora Nacional o poder de aprovar e impor medidas técnicas de execução, que aparecem no Regulamento 303/2019 da Autoridade Nacional de Comunicações (ANACOM), publicado a 1 de abril de 2019 em Diário da República. Esta legislação também impõe a comunicação de contato permanente, Responsável da Segurança, envio de relatório anual, análises de risco, Plano de segurança e obrigações de notificação das violações de segurança.

Existirão inclusive instituições que prestando serviços de telecomunicações, prestarão serviços digitais identificados no Anexo da Lei n.º 46/2018, e que assim terão obrigações de identificação, elaboração e reporte sobre segurança da informação e proteção de dados para com as três Autoridades distintas: CNPD, CNCS e ANACOM.

Entrevista a Luís Ferreira Mendes, Vogal da Direção da APDPO

Luís Ferreira Mendes
Consultor de proteção de dados
Sócio-gerente da Ferreira Mendes, Unipessoal Lda

Antes de mais, agradeço o convite feito pela Diretora da DPO Magazine, e Presidente da APDPO, Dr.ª Inês Oliveira, pelo gentil convite para prestar a presente entrevista! Que aproveite aos leitores, como aproveitou ao entrevistado o convite a recentrar em temáticas antigas e sempre novas.

Aceitou o desafio de integrar a direção da APDPO. Que mais valias vê nos projetos associativos?

Com surpresa e espírito de missão aceitei o convite que partiu da Dra. Inês Oliveira para integrar a sua lista aos órgãos sociais da APDPO para o mandato 2021-2024. Com surpresa por me tratar de um associado "discreto" mas presente, que vem perdido desde o Alentejo e que, na medida do possível, participava da vida da APDPO. O espírito de missão deriva da minha forma de estar pessoal e profissionalmente, entregue aos projetos que abraço, na procura por dar mais do que receber.

Acerca dos projetos associativos e, no caso concreto, da APDPO, fazem todo o sentido e cada vez mais, devendo ser estimados, apoiados, acarinhados e merecer o empenho de todos. Os projetos associativos, enquanto agregadores de iguais (ou por perseguirem um objetivo comum, que pode ser cultural, social, religioso ou profissional, ou por agremiarem a valorização e divulgação de determinadas funções sociais) na prossecução de objetos sociais definidos, constituem-se como a verdadeira "rede social" – desde sempre o foram, mas são hoje, mais do que nunca, numa aceção radical do termo.

Partindo da minha situação concreta, sempre a vida associativa esteve presente:

a participação no clube desportivo da freguesia, na sociedade musical e cultural, na associação de estudantes, desde o secundário até ao ensino superior, na militância política e na filiação religiosa. Embora em diferentes níveis, sempre a associação a outros, por comungar dos mesmos objetivos, fez sentido. Daí, falar na aceção radical da associação como a "rede social" por excelência.

Falar de mais valias associadas a projetos associativos pode trazer dois "pré-conceitos": os projetos associativos apenas consomem o dinheiro das quotas, oferecendo muito pouco aos associados; os projetos associativos, quando assumidos e no desempenho de missões sociais, como dirigente, consomem o bem mais escasso: o tempo! Destes dois "pré-conceitos" todos teremos provas, experiências e, nalguns casos, más recordações! Nada mais errado, naquilo que ao projeto associativo da APDPO diz respeito. Nunca senti, enquanto associado, que dava a minha quota à APDPO como mal entregue: sempre obtive elevado retorno, seja pela empatia, valorização e capacitação, pela aquisição de conhecimento e pela partilha de experiência. Agora, como diretor da APDPO não sinto que o tempo me seja "roubado": o tempo entregue para a gestão da vida associativa traz consigo o enorme retorno da valorização do associado e da dignificação da APDPO. Sentir que, no diálogo com parceiros, a APDPO é reconhecida na área, é respeitada pela sua ação associativa e pela defesa dos seus associados, é a prova de que o tempo "gasto", dedicado melhor dito, neste projeto associativo, tem o melhor retorno exigível.

Na sua opinião, que características essenciais tem que ter o profissional que quer entrar para o mercado da proteção de dados?

Mergulhando no objeto social que caracteriza a nossa APDPO, a formação dos profissionais e o seu reconhecimento, seria necessário delinearmos um "perfil" do profissional que queira entrar no mercado da proteção de dados: formação, informação, disposição e boa disposição!

Formação – o profissional que queira entrar no mercado da proteção de dados tem que apostar, seriamente, na formação. E essa formação tem que ser capacitante, desafiadora, transversal e permanente. Não basta que preencha um quadro formatado de competências, em determinada área, mas que seja sobretudo interessado e curioso, aberto à investigação e ao conhecimento de causa, no terreno, um "saber fazendo" e um "fazer sabendo" constante.

Informação – o profissional que queira entrar no mercado da proteção de dados tem que ter um gosto e interesse pela informação; devo fazer um alerta: um gosto e um interesse pela verdadeira, baseada e referenciada informação, assente em bases e fontes credíveis, provadas e testadas. A informação, como manancial dos nossos tempos, tem que ser ainda mais escrutinada. Não basta ao profissional (nem a ninguém) ter como fontes, sítios dúbios, fontes corporativas ou meras opiniões; deve ser o

profissional o primeiro a testar as suas fontes e a fazer sobre elas um exercício crítico. Desta necessidade de informação, decorrem também momentos de partilha e de troca de experiências, de permanente aquisição de conteúdo e de leitura crítica dos factos.

Disposição – o profissional que queira entrar no mercado da proteção de dados tem que se dispor a evangelizar tudo e todos à sua volta, para a importância e necessidade de uma cultura de proteção de dados, seja na organização onde desempenha funções, seja no ambiente empresarial onde quer desempenhar as suas funções, seja na comunidade onde vive e se movimenta, para criar essa verdadeira cultura de proteção de dados. Também quando falo em disposição, falo de "pré-disposição" para ser um profissional que quer entrar no mercado da proteção de dados: a "pré-disposição" de saber que nunca sabe tudo, a "pré-disposição" para ouvir muitas desconfianças, más experiências e dúvidas sobre a pertinência e ocasião do seu trabalho, a "pré-disposição" para ser um autêntico evangelizador da proteção de dados – fala de algo que muito poucos conhecem, a muito poucos interessados, com muito pouco tempo, com muito poucos recursos e que, sem saber, precisam muito da sua ajuda! A disposição do profissional deve ser, assim, fazer perceber e sentir a necessidade da proteção de dados no negócio, na organização e na cultura digital!

Boa disposição – por que com ela, tudo o que foi dito até aqui pode levar-se com otimismo, realismo e muita vontade!

Acha que as lideranças ao mais alto nível já estão comprometidas com a proteção de dados?

Nos tempos que correm, e mesmo nos tempos que já corriam, a proteção de dados não é um bom lugar para investir. Não é porque as organizações que, fruto das "modas" a ela se dediquem, arriscam a ter que alocar grandes verbas para verificar, aplicar e manter a conformidade; para organizações que assumam um compromisso com a cultura de proteção de dados, podem surgir custos que a reputação irá atenuar; para as empresas que, desde a génese, assumiram a proteção de dados como uma parcela do negócio, o custo/benefício já está resolvido.

O nosso tecido empresarial e organizacional (público/Estado ou privado/empresarial) não está, de todo, comprometido com a proteção de dados. Arrisco dizer que uma grande fatia das lideranças não está, sequer, consciente da importância. Pode ser uma análise simplista ou ignorante, mas é aquela que se sente no terreno. Alguns momentos, eventos ou acontecimentos trazem à efervescência dos dias a problemática da proteção de dados que a espuma dos dias acaba por esboroar. Para muitos, a proteção de dados é como um festival pirotécnico: desde que mantido longe da ignição, pode estar armazenado em local próprio ou impróprio, tanto faz, com condições ou sem elas… mas se a igni-

ção se aproxima e deflagra no material pirotécnico, assume luz e estrondo, que felizmente passa, deixando por vezes algum cheiro, mas sem incómodos de maior… Pode ser uma imagem simplista e ignorante, mas é aquela que se sente no terreno.

Mas nem tudo é assim, este não é o retrato homogéneo do nosso país! Felizmente! Todavia, creio que é o cenário que mais marca e ilustra o nosso país… Em alguns centros urbanos, por força do negócio ou da mobilidade do poder, esta temática pode estar mais presente e as lideranças mais sensibilizadas: e são cenários privilegiados, que devem ser divulgados e valorizados!

É neste cenário que a APDPO tem que assumir o seu papel de charneira na defesa, formação e promoção do profissional de proteção e segurança dos dados! Só com uma carreira assente no rigor, na atualização e na competência, só com profissionais ética e profissionalmente comprometidos, que conhecem a realidade da proteção de dados, que procuram saber e fazer mais e melhor, será possível despertar nas lideranças a consciência e o compromisso com a proteção de dados!

O que falta fazer para uma cultura de proteção de dados dos trabalhadores em geral?

A grande falha é na consciencialização generalizada da população para a cultura da proteção de dados. Apenas quando for transversal e "natural" a defesa e cuidado com a proteção de dados, teremos uma cultura de proteção de dados, quer nos trabalhadores/colaboradores, quer nos empregadores/dirigentes. Até lá, faremos sensibilizações extemporâneas, que podem dispor os ouvintes, mas que dificilmente comprometem.

Todavia, enquanto não vivemos uma verdadeira cultura de proteção de dados, existem momentos e eventos que podem sensibilizar para a importância da proteção de dados: formação teórica, formação em ambiente laboral, simulações e testes, momentos lúdicos ou de lazer em empresa dedicados a esta temática, enfim. Não nos faltem ideias, que a sensibilização não tem limites!

Sendo este um espaço e um canal para profissionais da área da proteção de dados, reforço a mensagem de que a sensibilização tem que ser permanente, evolutiva e dinâmica. Aproveitemos o nosso convívio familiar e comecemos já a evangelizar para o tema; aproveitemos o convívio laboral/profissional para sensibilizar para o tema; aproveitemos os momentos de consumo, de participação ativa na vida social, cultural ou política para sensibilizar para o tema! O tema da proteção de dados não pode ficar relegado ao gueto da ignorância e do obscurantismo! O tema da proteção de dados tem que sair para a luz do dia, ser assumido como uma parte fundamental da formação cívica das gerações e, só assim, a vida do profissional de proteção de dados terá um autêntico sentido!

A Denúncia e os trabalhadores

Maria Graça M. Casimiro Almeida
DPO
PROLEITE, CRL.

A prática de irregularidades organizacionais prejudica os direitos e os benefícios dos funcionários, da organização e do público em geral. A denúncia de irregularidades foi usada pela primeira vez como um conceito num documento legal em 1963 (Kozak e Şahin, 2018). A denúncia é a divulgação de irregularidades por membros atuais ou ex-membros da organização, tais como: práticas ilegais, imorais ou ilegítimas (Near e Miceli, 1985). De acordo com Treviño, et al., 2006 é uma característica organizacional autónoma de comportamentos pró-ativos, pró-sociais e éticos. A denúncia é um dos principais mecanismos no combate à corrupção, fraude e crimes. Desempenha um papel relevante no que toca à deteção destes crimes, devido à sua essência. A denúncia identifica-se tanto para o setor público como para o privado. Contudo, a legislação de 2008 (Lei 19/2008, de 21 abril) que é aplicável apenas ao setor público e de forma vaga e sem regulamentação específica, não exerce o seu vínculo na totalidade, permanecendo até agora um conjunto de instrumentos legislativos que não garante segurança e que se faça a devida justiça (TIAC, 2013).

A denúncia pode ocorrer sobre duas maneiras: a interna e a externa. Isto no que trata à divulgação de informação privilegiada relativamente a práticas incorretas, na forma escrita ou verbal, pelo funcionário da organização ao seu próprio diretor e à sua gestão de topo e ou aos auditores da empresa (Celep e Konaklı, 2012; Nayir e Herzig, 2012). O processo de denúncia de irregularidades é mais bem utilizado pelos departamentos de auditoria interna das empresas, atuando de imediato com as medidas ne-

cessárias (Schneider, 2008). A denúncia interna de irregularidades pode beneficiar a organização uma vez que oferece oportunidades de autocorreção para problemas antiéticos (Miceli et al., 2009). Pelas denúncias externas, a divulgação de atos ilícitos de pessoas ou autoridades externas à organização, podem fazer constrangimentos públicos e provocarem fiscalizações governamentais, multas pesadas e litígios (Berry, 2004). Pesquisas demonstraram que denúncias internas na China são especialmente difíceis porque geralmente são interpretadas como o desafiar da estrutura de poder da organização ou questionar mesmo a gestão de topo, refletindo um problema de hipersensibilidade na sua cultura, trazendo implicações teóricas e práticas especiais (Zhou, et al., 2018)

A denúncia de irregularidades é um tópico significativo na gestão da ética organizacional, que se preocupa na forma como os funcionários estão dispostos a denunciar, assim como na criação de mecanismos que incutam esse comportamento. Miceli et al., (2009) advogam que a potencial retaliação enfrentada pelos denunciantes, na sua maioria funcionários, existe, pelo que alguns funcionários não estão dispostos a denunciar as irregularidades dos colegas, resultando na perda de oportunidades de autocorreção das suas irregularidades, contribuindo assim para o comprometimento da reputação, assim como na incorreção de custas judiciais.

Os avanços de estudos académicos trouxeram evidência de algumas características pessoais particulares que influenciam a tomada de decisão sobre denúncias, tais como: a personalidade, a personalidade proactiva, a autoeficácia, a relevância específica da situação e as diferentes características demográficas (MacNab e Worthley, 2008; Rehg, et al., 2008; Bjørkelo, et al., 2010; Miceli, et al., 2012; Liu, et al., 2016).

Fatores organizacionais, como a liderança ética, a liderança transformacional, a validação dos colegas de trabalho, a cultura ética, a cultura de comunicação, as regras de trabalho em equipa e suporte organizacional, têm demonstrado desempenhar papéis importantes no âmbito pessoal na tomada de decisão do denunciante (Keenan, 2002; Tavakoli, et al., 2003; Edwards, et al., 2009; Skivenes e Trygstad, 2010; Kaptein, 2011; Caillier, 2013; Latan, et al., 2017).

A cultura ética ajuda os funcionários a interpretarem a recompensa e apoio da organização relativamente à ética e aos elementos que constituem um comportamento adequado e desejado (Arnaud e Schminke, 2012). Desta forma, pode impedir a realização de atos antiéticos e aumentar a disposição dos funcionários em falarem sobre problemas organizacionais (Wang e Hsieh, 2013). Uma cultura ética forte significa que a organização está preocupada com o bem-estar dos funcionários na busca de compromissos organizacionais, atribuindo importância a crenças morais pessoais, às leis e códigos de conduta nas tomadas de decisão e pode construir normas positivas de denúncia (Martin e Cullen, 2006). Quando os funcionários percebem a existência duma cultura ética forte acreditam que a denúncia das irregularidades é bem-vinda pela

administração, onde a organização elogia, valoriza e recompensa o denunciante e considera a denúncia como um contributo do funcionário (Leung, 2008). Numa perspetiva de troca social, a forte cultura ética permite que os funcionários sintam a preocupação da organização com os interesses dos funcionários, trazendo melhoria no aspeto psicológico dos funcionários e compromissos organizacionais, preservando a organização de atos ilícitos, demonstrando lealdade. Kaptein (2011) mostrou que uma cultura ética positiva antecipou a intenção dos funcionários nas denúncias internas. Zhang, et al. (2009) mostraram que uma cultura ética melhora a relação entre o julgamento ético e a intenção de denúncia interna por parte do funcionário. Contrariamente, uma cultura ética fraca pode levar os funcionários a um julgamento de comportamento ético incorreto, encapotando situações de transgressões e procura de justificação para o sucedido, implicando numa indiferença da administração.

Segundo Keil, et al., (2010) fatores individuais e contextuais influenciam as irregularidades dos observadores na avaliação dos custos (represália e intimidação no local de trabalho) e dos benefícios (cessação de irregularidades e recebimento de recompensa) na tomada de medidas sobre denúncias.

Funcionários com grande sentido de pertença organizacional tendem a agir em favor dos interesses da organização, em vez dos seus próprios (Riketta, 2005), e funcionários com grande identidade moral tendem a agir de maneira "certa" ou "moral", independentemente dos resultados da ação (Reed e Aquino, 2003).

As pesquisas de Mesmer-Magnus e Viswesvaran, (2005); Miceli, et al., (2008); Henik, (2015) refletem que o receio da retaliação é preocupante para potenciais denunciantes e evitar a retaliação é um tema relevante em conselhos sobre denúncias e sites de defesa dos direitos. Deve notar-se que os potenciais denunciantes têm intenções diferentes nas escolhas dos canais de apresentação de denúncia, dependendo do contexto vivenciado (Nayır et al., 2016). O processo de tomada de decisão das denúncias de irregularidades compreende quatro etapas básicas: observar as irregularidades na organização, analisar e julgar a situação, formar uma intenção de denúncia e informar (Dozier e Miceli, 1985; Gundlach, et al., 2003).

Bjørkelo e Bye (2014) concluíram que a intenção das denúncias dos funcionários é menos sensível, do que as outras etapas, não apenas porque os verdadeiros observadores ou denunciantes podem relatar a sua disposição para denunciar. A denúncia de irregularidades tem riscos potenciais pessoais e organizacionais. Por exemplo, expor uma irregularidade organizacional pode colocar em causa a capacidade de gestão, desafiando a hierarquia estabelecida e o poder dos líderes, opondo-se às rotinas da organização (Miceli, et al., 2008). A denúncia de irregularidades pode criar um clima de suspeita, de agressividade numa organização, desmoronando a identificação do grupo de funcionários, a lealdade e moral, acarretando um alto nível de risco pessoal e

influenciando de forma negativa o desempenho organizacional. Li, et al. (2016), fornece evidências em que a repugnância ao risco reduz o efeito da identificação dos funcionários da organização que assumem determinados riscos.

A criação e a manutenção de uma cultura ética forte são metas abrangentes de longo prazo. As políticas de recursos humanos podem apoiar o seu desenvolvimento, criando estratégias relevantes para encorajar a ética comportamental e punir o comportamento antiético, informando normas e orientações organizacionais aos funcionários por meio de ações de formação, incentivando os funcionários a comunicarem de forma livre expressando as suas opiniões e comentários críticos, assim como avaliar e promover os funcionários de acordo com o seu desempenho no trabalho, bem como a moralidade comportamental (Skivenes e Trygstad, 2010, 2017). Neste âmbito os gestores devem atuar como modelos éticos, estando patentes nas suas atitudes e comportamentos contribuindo para o aumento de confiança dos funcionários em prol da justiça organizacional (Miceli, et al., 2009).

McKenna et al., (2016); Stansbury e Victor (2008) encontram evidências dos efeitos de género, em que as mulheres são mais propensas a relatar os fatos do que homens, o tamanho da organização, em que as organizações mais pequenas são menos propensas do que as maiores no relato, os efeitos de posse, a presença e duração dum grupo de trabalho, tendem a reduzir a probabilidade de denúncia ao longo do tempo. Fieger, P. e Rice (2018) demonstram que em certos grupos profissionais, como no campo jurídico, da comunicação, do marketing e da tecnologia de informação, os níveis de relato são mais baixos e sugerem a implementação de uma política específica de desenvolvimento para apoiar a denúncia de irregularidades entre esses trabalhadores. Evidenciaram também que trabalhadores potencialmente marginalizados na organização, ou em que exista a barreira da língua tendem a ser menos propensos à denúncia.

Apoiar os denunciantes é um desafio importante para todas as organizações. As organizações devem instituir um sistema de denúncia visível para fornecer canais de denúncia confidenciais e convenientes (Miceli, et al., 2008), motivando os denunciantes a usá-los, dando incentivos financeiros e envidar esforços para garantir a segurança dos denunciantes para qualquer retaliação subjacente (Miceli, et al., 2009).

A construção de uma política de denúncia adequada promove a confiança, mas este efeito é limitado se os líderes não reforçarem o comportamento ético (Lewis 2011). Uma liderança positiva pode desempenhar um papel crítico na promoção de denúncias, pois evidencia a voz da consciência e do comportamento ético pró-social (Nayir e Herzig 2012). Estudos mostram que tanto a liderança transformacional quanto a ética podem favorecer atitudes e comportamentos de denúncias (Bhal e Dadhich 2011; Caillier 2013). Os funcionários que confiam nos líderes são mais inclinados a relatar as irregularidades aos seus

líderes ou organizações do que aqueles quem não confiam (Berry 2004).

Tem havido uma falta de compreensão sobre os efeitos das dimensões culturais específicas sobre fraude e denúncias, que levou a prevenções e mesmo deteções ineficazes (Cheng, et al., 2015; Liu, et al., 2015; Trongmateerut e Sweeney, 2013). Diferenças culturais podem influenciar a prática e a perceção de denúncia de fraude (Bierstaker, 2009). No entanto, existe algumas lacunas na literatura focadas nas respostas culturais globais para a denúncia de irregularidades (Albrecht et al., 2015; Henik (2015). O efeito externo da fraude também pode levar a uma perceção negativa por parte dos stakeholders que acreditam que a falta de mecanismos de controlos internos permita o seu surgimento (Liu, et al., 2016; McMahon, Pence, Bressler e Bressler, 2016; Peters e Maniam, 2016). A denúncia de irregularidades pode ser usada como método de deteção de fraudes. Os líderes organizacionais de todo o mundo têm cada vez mais desafios para reduzir ou eliminar atividades fraudulentas (Kaplan, et al., 2010; Mangala e Kumari, 2017; Segal, 2016). Além disso, a globalização gerou a necessidade duma avaliação dos ambientes sociais onde estão inseridos os colaboradores e as organizações (Beugelsdijk, et al., 2015; Drnevich e Stuebs, 2013). Para que as políticas de denúncia de irregularidades sejam eficazes, estas devem ser adaptadas a culturas organizacionais e individuais uma vez que uma política padrão pode ser mais eficaz em algumas organizações comparativamente com outras (Loyens, 2013).

Mihret (2014) identificou três dimensões culturais que estão intimamente relacionadas com irregularidades, a distância do poder, a prevenção da incerteza e o individualismo / coletivismo. Todas as linhas de comunicação na organização devem ser abertas. A gestão, os funcionários podem criar um sistema para receber notificações. As pessoas que trabalharem nesse processo devem ser confiáveis e ter habilidades de comunicação eficazes e com sensibilidade ética. É extremamente importante ser feito de pessoas e para pessoas. Aqui todos os funcionários são iguais, graças às denúncias internas, e ao mesmo tempo, cada um assume a missão de supervisionar o seu colega; manter o anonimato é importante, a menos que o denunciante solicite o contrário; medidas eficazes devem ser tomadas para ocultar as suas identidades, sendo que esta garantia deve ser dada aos funcionários; potenciar seminários e conferências sobre estas matérias devem ser organizados e a sensibilidade dos funcionários para estas questões deve ser reforçada. Potipiroon e Wongpreedee (2021) concluíram que os seus resultados revelam que a complexidade do processo de denúncia depende em parte do tipo de canais de denúncia utilizados na pesquisa.

Hoje os funcionários denunciantes são apreciados e em muitos países são protegidos por leis para evitar retaliações (Nayir e Herzig, 2012), contudo no nosso país não existe legislação para assegurar estas situações de forma plena. Tudo ainda está muito vago. Assim, deverá ser um caminho a percorrer pela investigação destas matérias,

tão importante para os funcionários e para a reputação corporativa, para que o princípio da transparência e da abertura reduza a tendência de ocultação de imprecisões articulado com o código de conduta das organizações.

Referências bibliográficas

Albrecht, C., Holland, D., Malagueño, R., Dolan, S., & Tzafrir, S. (2015). The role of power in financial statement fraud schemes. Journal of Business Ethics, Vol. 131, No.4, pp. 803-813.

Arnaud, A. and Schminke, M. (2012). The ethical climate and context of organizations: a comprehensive model. Organization Science, Vol. 23 No. 6, pp. 1767-1780.

Berry, B. (2004). Organizational culture: a framework and strategies for facilitating employee whistle blowing. Employee Responsibilities and Rights Journal, Vol. 16, No. 1, pp. 1-11.

Beugelsdijk, S., Maseland, R., and Van Hoorn, A. (2015). Are scores on Hofstede's dimensions of national culture stable over time? A cohort analysis. Global Strategy Journal,Vol. 5, No.3, pp. 223- 240.

Bierstaker, J. L. (2009). Differences in attitudes about fraud and corruption across cultures. Cross Cultural Management, Vol. 16, No. 3, pp. 241-250.

Bhal, K. T., and Dadhich, A. (2011). Impact of ethical leadership and leader–member exchange on whistle blowing: The moderating impact of the moral intensity of the issue. Journal of Business Ethics, Vol. 103, No. 3, pp. 485–496.

Bjørkelo, B. and Bye, H.H. (2014). On the appropriateness of research design: Intended and actual whistleblowing. in Brown, A.J., Moberly, R.E., Lewis, D. and Vandekerckhove, W. (Eds), International Handbook On Whistleblowing Research, Edward Elgar, Cheltenham, pp. 133-153.

Bjørkelo, B., Einarsen, S. and Matthiesen, S.B. (2010). Predicting proactive behavior at work: exploring the role of personality as an antecedent of whistle blowing behavior, Journal of Occupational and Organizational Psychology, Vol. 83 No. 2, pp. 371-394.

Caillier, J.G. (2013). Transformational leadership and whistle-blowing attitudes: is this relationship mediated by organizational commitment and public service motivation?. American Review of Public Administration, Vol. 45 No. 4, pp. 458-475.

Celep, C. and Konaklı, T. (2012). Bilgi İfşası: Eğitim Örgütlerinde Etik Ve Kural Dışı Uygulamalara Yönelik Bir Tepki. E- International Journal Of Educational Research, Vol. 3, No. 4, pp. 65-88.

Cheng, X., Karim, K. E., & Lin, K. J. (2015). A cross-cultural comparison of whistleblowing perceptions. International Journal of Management & Decision Making, Vol.14, No 1, pp. 15-31.

Dozier, J.B. and Miceli, M.P. (1985). Potential predictors of whistle-blowing: a prosocial behaviour perspective. Academy

of Management Review, Vol. 10 No. 4, pp. 823-836.

Drnevich, D., & Stuebs, M. (2013). Cultural differences and judgment in financial reporting standards. Journal of Accounting Education, Vol. 31, No 4, pp. 461-482.

Edwards, M., Ashkanasy, N.M. and Gardner, J. (2009). Deciding to speak up or to remain silent

following observed wrongdoing: the role of discrete emotions and climate of silence. in Greenberg, J. and Edwards, M. (Eds), Voice and Silence in Organizations, Emerald Group Publishing, Bingley, pp. 83-109.

Fieger, P. and Rice, B. (2018). Whistleblowing in the Australian Public Service: The role of employee ethnicity and occupational affiliation. Personnel Review.Vol. 47, No. 3, pp. 613–629.

Gundlach, M.J., Douglas, S.C. and Martinko, M.J. (2003). The decision to blow the whistle: a social information processing framework. Academy of Management Review, Vol. 28 No. 1, pp. 107-123.

Henik, E. (2015). Understanding whistleblowing: a set-theoretic approach. Journal of Business Research, Vol. 68 No. 2, pp. 442-450.

Kaplan, S. E., Pope, K. R., and Samuels, J. A. (2010). The effect of social confrontation on individuals' intentions to internally report fraud. Behavioral Research in Accounting, Vol.22, No. 2, pp. 51-67.

Kaptein, M. (2011). From inaction to external whistle blowing: the influence of the ethical culture of organizations on employee responses to observed wrongdoing. Journal of Business Ethics, Vol. 98, No. 3, pp. 513-530.

Keenan, J.P. (2002). Whistleblowing: a study of managerial diferences. Employee Responsibilities and Rights Journal, Vol. 14 No. 1, pp. 17-32.

Kozak, Meryem Akoğlan- Şahin, Sibel (2018). Bilgi İfşası (Whistleblowig) Ve Etik İkilem Üzerine Çıkarımlar. Anatolia Turizm Araştırmaları Dergisi, Vol. 29, No.1, pp.31-38.

Latan, H. and Jabbour, C.J.C. (2017). Ethical awareness, ethical judgment and whistleblowing: a moderated mediation analysis. Journal of Business Ethics, No. 1, pp. 1-16.

Leung, A.S.M. (2008). Matching ethical work climate to in-role and extra-role behaviors in a collectivist work setting. Journal of Business Ethics, Vol. 79 Nos. 1/2, pp. 43-55.

Lewis, D. (2011). Whistleblowing in a changing legal climate: Is it time to revisit our approach to trust and loyalty at the workplace? Business Ethics, Vol.20, No.1, pp. 71–87.

Li, R., Zhang, Z.Y. and Tian, X.M. (2016). Can self-sacrificial leadership promote subordinate taking charge? The mediating role of organizational identification and the moderating role of risk aversion. Journal of Organizational Behavior, Vol. 37 No. 5, pp. 758-781.

Liu, Y., Zhao, S., Jiang, L. and Li, R. (2016). When does a proactive personality enhance an employee's whistle-blowing intention? A cross-level investigation of the employees in Chinese companies.

Ethics & Behavior, Vol. 16 No. 1, pp. 660-677.

Liu, S., Liao, J., and Wei, H. (2015). Authentic leadership and whistleblowing: Mediating roles of psychological safety and personal identification. Journal of Business Ethics, Vol. 131, No 1, pp. 107- 119.

Loyens, K. (2013). Towards a custom-made whistleblowing policy. Using grid-group cultural theory to match policy measures to different styles of peer reporting. Journal of Business Ethics, Vol. 114, No.2, pp. 239-249.

McKenna, B., Verreynne, M.L. and Waddell, N. (2016). Locating gendered work practices: a typology. International Journal of Manpower, Vol. 37 No. 6, pp. 1085-1107.

McMahon, R., Pence, D., Bressler, L., & Bressler, M. (2016). New tactics in fighting financial crimes: Moving beyond the fraud triangle. Journal of Legal, Ethical & Regulatory, Vol. 19, No.1, pp.16.

MacNab, B.R. and Worthley, R. (2008). Self-efficacy as an intrapersonal predictor for internal whistleblowing: a US and Canada examination. Journal of Business Ethics, Vol. 79 No. 4, pp. 407-421.

Mangala, D., & Kumari, P. (2017). Auditors' perceptions of the effectiveness of fraud prevention and detection methods. Indian Journal of Corporate Governance, Vol.10, No. 2, pp.118.

Martin, K.D. and Cullen, J.B. (2006). Continuities and extensions of ethical climate theory:

a meta-analytic review. Journal of Business Ethics, Vol. 69 No. 2, pp. 175-194.

Mesmer-Magnus, J.R. and Viswesvaran, C. (2005), "Whistle blowing in organizations: an examination of correlates of whistle blowing intentions, actions, and retaliation". Journal of Business Ethics, Vol. 62 No. 3, pp. 277-297.

Miceli, M.P., Near, J.P. and Dworkin, T.M. (2008). Whistle-blowing in Organizations, Routledge, New York, NY.

Miceli, M.P., Near, J.P. and Dworkin, T.M. (2009). A word to the wise: how managers and policy-makers can encourage employees to report wrongdoing. Journal of Business Ethics, Vol. 86 No. 3, pp. 379-396.

Miceli, M.P., Near, J.P., Rehg, M.T. and Van Scotter, J.R. (2012). Predicting employee reactions to perceived organizational wrongdoing: demoralization, justice, proactive personality, and

whistle-blowing. Human Relations, Vol. 65 No. 8, pp. 923-954.

Mihret, D. G. (2014). National culture and fraud risk: Exploratory evidence. Journal of Financial Reporting & Accounting, Vol.12, No.2, pp. 161-176.

Nayır, D.Z., Rehg, M.T. and Asa, Y. (2016). Influence of ethical position on whistleblowing behaviour: do preferred channels in private and public sectors differ?. Journal of Business Ethics, pp. 1-21.

Nayir, Dilek Z.- Herzig, Christian (2012). Value Orientations As Determinants Of Preference For External And Anonymous Whistleblowing. Journal Of Business Ethics, Vol. 107, pp.197-213.

Near, J.P. and Miceli, M.P. (1985). Organizational dissidence: the case of whistle-

blowing. Journal of Business Ethics, Vol. 4 No. 1, pp. 1-16.

Peters, S., and Maniam, B. (2016). Corporate fraud and employee theft: Impacts and costs on business. Journal of Business & Behavioral Sciences, Vol. 28, No.2, pp.104.

Potipiroon W. and Wongpreedee A. (2021). Ethical Climate and Whistleblowing Intentions: Testing the Mediating Roles of Public Service Motivation and Psychological Safety among Local Government Employees. Public Personnel Management, Vol.50, No.3, pp. 355-.

Reed, A.II. and Aquino, K.F. (2003). Moral identity and the expanding circle of moral regard toward out-groups. Journal of Personality & Social Psychology, Vol. 84 No. 6, pp. 1270-1286.

Rehg, M.T., Miceli, M.P., Near, J.P. and Van Scotter, J.R.V. (2008). Antecedents and outcomes of retaliation against whistleblowers: gender differences and power relationships. Organization Science, Vol. 19 No. 2, pp. 221-240

Riketta, M. (2005). Organizational identification: a meta-analysis. Journal of Vocational Behavior, Vol. 66 No. 2, pp. 358-384.

Schneider, Arnold (2008). The Roles Of Internal Audit In Complying With The SarbanesOxley Act. International Journal Of Disclosure And Governance, Vol.6, No. 1, pp.69-79.

Segal, S. Y. (2016). Accounting frauds - review of advanced technologies to detect and prevent frauds. Economics & Business Review, Vol.2, No. 4, pp. 45.

Skivenes, M. and Trygstad, S. (2017). Explaining whistle-blowing processes in the Norwegian labour market: between individual power resources and institutional arrangements. Economic and Industrial Democracy, Vol. 38 No. 1, pp. 119-143.

Skivenes, M. and Trygstad, S.C. (2010). When whistle-blowing works: the Norwegian case.

Human Relations, Vol. 63 No. 7, pp. 1071-1097.

Stansbury, J.M. and Victor, B. (2008). Whistle-blowing among young employees: a life-course perspective. Journal of Business Ethics, Vol. 85 No. 3, pp. 281-299.

Tavakoli, A.A., Keenan, J.P. and Cranjak-Karanovic, B. (2003). Culture and whistleblowing an empirical study of Croatian and United states managers utilizing Hofstede's cultural dimensions. Journal of Business Ethics, Vol. 43 Nos 1/2, pp. 49-64.

TIAC 2013 - Uma Alternativa ao Silêncio: A proteção de denunciantes em Portugal, fevereiro 2013, disponível em: https://transparencia.pt/wp-content/uploads/2013/11/WB-PT-FINALL.pdf

Treviño, L.K., Weaver, G.R. and Reynolds, S.J. (2006). Behavioural ethics in organizations: a review. Journal of Management, Vol. 32 No. 6, pp. 951-990.

Trongmateerut, P., and Sweeney, J. (2013). The influence of subjective norms on whistle-blowing: a cross-cultural investigation. Journal of Business Ethics, Vol.112, No. 3, pp. 437-451.

Wang, Y.D and Hsieh, H.H. (2013). Organizational ethical climate, perceived organizational support, and employee silence: a cross-level investigation. Human Relations, Vol. 66 No. 6, pp. 783-802.

Zhang, J., Chiu, R. and Wei, L. (2009). Decision-making process of internal whistleblowing behavior in China: empirical evidence and implications. Journal of Business Ethics, Vol. 88 No. 1, pp. 25-41.

Zhou, L., Liu, Y., Chen, Z., Zhao, S. (2018). Psychological mechanisms linking ethical climate to employee whistle-blowing intention. Journal of Managerial Psychology, Vol. 33, No.2, pp. 196–213.

Canais de denúncia

Anabela Pais
DPO
Ascendi

1. Enquadramento legal

A Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019 (Diretiva *Whistleblower* doravante, Diretiva), relativa à proteção das pessoas que denunciam violações do direito da União, veio instituir um regime geral de proteção dos denunciantes assente em duas orientações fundamentais: o estabelecimento de canais de denúncia e a proibição de quaisquer atos de retaliação.

É propósito deste artigo abordar o tópico relativo aos canais de denúncia, à luz dos requisitos previstos na referida Diretiva.

2. Canais de denúncia

A Diretiva obriga à implementação de canais e procedimentos de denúncia interna que garantam a confidencialidade e segurança das informações recebidas.

Esta obrigação é aplicável tanto às entidades do setor público como do setor privado com 50 ou mais trabalhadores, sem prejuízo de exceção a identificar pelo Estado-membro, nomeadamente no caso de municípios com menos de 10.000 habitantes.

Os requisitos que devem ser seguidos pelos canais e procedimentos de denúncia são:

i. Canais seguros que garantam a confidencialidade da identidade dos denunciantes e dos terceiros mencionados na denúncia, com vista a impedir o acesso não autorizado a essa informação;

ii. Avisos de receção da denúncia ao denunciante num prazo de 7 dias a contar da data da receção;

iii. A designação de uma pessoa ou serviço imparcial competente para dar seguimento às denúncias e que ficará encarregue por manter a comunicação com o denunci-

ante e, se necessário, solicitar informações complementares e dar feedback ao denunciante.

A Diretiva determina ainda que os Estados-membros devem designar autoridades competentes que estabeleçam canais de denúncia externa independentes e autónomos que possam acolher e tratar as denúncias que lhes sejam dirigidas.

Em analogia ao que se verifica para os canais internos, também no caso das denúncias externas são definidos um conjunto de requisitos, inclusivamente que o pessoal responsável pelo tratamento receba formação específica para o efeito.

A Diretiva orienta os Estados-membros a promoverem os canais internos de denúncia, devendo estes ter precedência sobre os canais externos. De todo o modo, ficará sempre ao critério do denunciante a opção quanto ao canal de denúncia.

3. Formas de denúncia

Os canais de denúncia devem possibilitar a comunicação de denúncias por escrito ou verbalmente ou por ambas as formas. A denúncia verbal deve ser permitida através de telefone ou através de outros sistemas de mensagem de voz ou, caso tal seja solicitado pelo denunciante, em reunião presencial.

4. Articulação com o RGPD

Os tratamentos de dados pessoais a efetuar ao abrigo da Diretiva devem observar as regras previstas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (RGPD), conforme previsto no Considerando 83 e Artigo 17º da Diretiva. Por conseguinte, qualquer tratamento de dados neste contexto deverá respeitar os princípios da legitimidade do tratamento, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação e segurança.

A segunda parte do Artigo 17º da Diretiva prevê também que quaisquer dados pessoais que não sejam relevantes para o tratamento de uma denúncia específica não devem ser recolhidos. Se recolhidos, tais dados devem ser apagados sem demora injustificada.

Além disso, sublinha-se aqui as obrigações de confidencialidade e segurança dos tratamentos dos dados que estão em linha com o preconizado no RGPD e se revelam quesitos essenciais para garantir a eficácia dos sistemas de denúncia.

5. Proposta de lei e parecer CNPD

O prazo de transposição da Diretiva para a legislação nacional termina a 17 de dezembro de 2021, existindo já uma iniciativa legislativa nesse sentido identificada por Proposta de Lei n.º 91/XIV/2ª.

A Comissão Nacional de Proteção de Dados (CNPD) foi convocada a emitir parecer sobre a dita Proposta de Lei, o que o fez através do seu Parecer 2021/76, de 9 de junho p.p., do qual se realça uma das recomendações que versa sobre a redação do Artigo 18.º relativo ao "Tratamento de dados pessoais".

Atendendo, por um lado, ao postulado nesse artigo relativamente à proibição de recolha dos dados pessoais que manifestamente não forem relevantes para o tratamento da denúncia e, por outro lado, à manifesta impossibilidade de evitar a recolha e/ou o apagamento desses dados em determinadas circunstâncias, por exemplo no caso do canal telefónico, a CNPD recomenda a revisão do n.º 2 nos seguintes moldes: *"Os dados pessoais manifestamente irrelevantes para o tratamento da denúncia não devem ser recolhidos e, tendo em conta o canal de denúncia utilizado, quando tal não seja possível, devem ser apagados sem demora e não podem ser considerados."*

Ficamos, assim, na expectativa relativamente ao texto final da Lei de transposição da Diretiva, o qual merecerá certamente uma nova e aprofundada reflexão!

A Epidemia pelo Vírus SARS-CoV-2 e as infrações ao RGPD por ela disseminadas

André de Sousa-Dias
Farmacêutico

A 11 de Março de 2020, a Organização Mundial de Saúde, declarava que o Vírus SARS-CoV-2, que tinha emergido na China em finais de 2019, se tinha precipitado e gerado uma situação pandémica.

Por cá, desde meados de Fevereiro de 2020, a comunicação social relatava a situação que se estava a viver por esses dias, em Itália, mais concretamente na zona norte de Itália, na pequena cidade de Codogono (1).

Naturalmente que as imagens e os relatos vindos de Itália geraram um progressivo sentimento de temor que se vivia por esses dias apesar de até ao momento não haver casos, mas era expectável que tal não se manteria.

Uns dias após as notícias dos primeiros casos, o Presidente da República anunciou a 18 de Março a declaração do estado de emergência (2).

Em simultâneo, a Direção Geral da Saúde (DGS) e o Governo encetaram uma série de medidas excepcionais e começou-se a ouvir falar da monitorização da temperatura corporal e outros dados de saúde, generalizadamente e nos locais de trabalho como forma de combate à epidemia que se alastrava pelo País.

Na nossa sociedade, sabemos ainda que a cultura social do medo predomina face à responsabilidade, ou outras características dos nossos concidadãos.

Assim talvez não tenha sido uma estranheza, que nesse ambiente fosse quebrado o elo que só Médicos, Farmacêuticos, Enfermeiros, e demais pessoal qualificado que exercem profissão na área da Saúde humana, tivessem acesso aos dados de saúde, conforme o disposto no artigo 9º do RGPD.

Importava, assim, recordar e esclarecer que os dados pessoais relativos à saúde são dados sensíveis, reveladores de aspectos da vida privada do cidadão e, em princípio, não têm que ser do conhecimento de pessoas ou entidades para lá do seu profissional de saúde, ou autoridades de saúde, no âmbito da saúde pública.

Nem devem sê-lo por poderem gerar ou potenciar discriminação. É por essa razão que esta categoria de dados está sujeita a um regime jurídico especialmente reforçado de proteção de dados. (3)

Foi incontável as vezes em que se assistiu à monitorização da temperatura corporal, até para entrar num estabelecimento de saúde pública, se passava a ser controlado pela segurança, quando um utente iria ter uma consulta com o seu médico.

Para lá disso há provas que foi frequente as entidades patronais terem tido conhecimento dos resultados dos testes à covid-19 dos seus trabalhadores, sendo decerto que alguns, não surpreenderia se tivessem achado no papel da sua interpretação, conforme os resultados e os seus próprios interesses, podendo ou não ter havido violação das normas que prevêem o isolamento dos casos suspeitos.

Por outro lado e em consequência da vontade colectiva, que só podemos louvar de combate à infeção pelo Vírus SARS-CoV-2, generalizou-se a solicitação de testes especialmente quando os denominados testes rápidos ficaram disponíveis em Outubro de 2020 (4).

Contudo veio-se a saber que os resultados destes foram frequentemente disponibilizados à entidade que os solicitou e comparticipou.

Soube-se, assim, que houve inúmeras entidades do setor privado e público que obtiveram conhecimento ilegítimo dos resultados dos testes. No entanto, foram mais noticiadas as violações promovidas por entidades públicas. (5)

Acresce que esta situação se amplificou no período que decorreu no Outono / Inverno de 2020.

A decisão do Legislador, no Decreto-Lei n.º 8/2020, que executou o novo estado de emergência decretado pelo Presidente da República, estilhaçou o equilíbrio de Direitos fundamentais contraditórios, ao optar pela salvaguarda da Saúde Pública e omitindo outros aspetos (6).

Este Diploma promoveu diversas medidas e procurou generalizar a capacidade de testagem, podendo em alguns casos contrariar a vontade do titular. Por outro lado, procurou-se reforçar e justificar a ausência da pessoa, no seu local de trabalho ou em locais públicos, por possuir uma temperatura corporal superior a 38.ºC, o que consubstanciava a possibilidade de estar infectado (6).

A falta de consenso dentro da comunidade científica e de profissionais de saúde, não pode, todavia, justificar uma generalização de medidas arbitrárias, tanto mais que as matérias de Saúde Pública e individual são complexas e houve, a meu ver, uma excessiva simplificação.

Hoje sabe-se, contudo, que estas medidas não acutelaram a necessidade de um novo confinamento geral, que era o objectivo do novo estado de emergência (6).

Foi um período extraordinário, mas se a situação sanitária, impunha medidas de salvaguarda por parte do Estado, para que a capacidade de resposta do Serviço Nacional de Saúde (SNS) não se esgotasse, negligenciou-se a promoção de uma política mais eficaz na articulação, entre os diversos Profissionais de Saúde, devidamente qualificados.

Decerto que houve pessoas que se sentiram estigmatizadas, em consequência do pouco cuidado pela parte dos responsáveis pelo tratamento dos dados (5,7).

Acresce que esta matéria foi relegada para segundo plano, já que a capacidade fiscalizadora divulgada, até ao momento, saldou-se por uma coima atribuída, a uma autarquia no montante de 2500,00 € (8).

Sem prejuízo das orientações e inúmeros pareceres que a CNPD, emitiu, e da voz pública, por meio da sua Presidente, em Janeiro de 2021, em que expressou muitas destas preocupações, será o prelúdio de uma acção fiscalizadora mais efectiva? (5)

Bibliografia citada:

1. Marymount International School. Italy: Codogno covid-free for first time since February 2020 [Internet]. 16-julho de 2021. 2021 [citado 14 de Setembro de 2021]. Disponível em: https://www.wantedinrome.com/news/italy-codogno-covid-free-for-first-time-since-february-2020.html
2. Presidente da República. Mensagem-do-Presidente-da-República-ao-País-sobre-a-declaracao-do-estado-de-emergencia [Internet]. 18-03-2020. [citado 14 de Setembro de 2021]. Disponível em: https://www.presidencia.pt/atualidade/toda-a-atualidade/2020/03/mensagem-do-presidente-da-republica-ao-pais-sobre-a-declaracao-do-estado-de-emergencia/
3. Comissão Nacional de Protecção de Dados. Orientações sobre recolha de dados de saúde dos trabalhadores. Vol. 2016. LISBOA; 2020.
4. DGS, INFARMED, INSA. Circular Informativa Conjunta [Internet]. 2020. p. 1–10. Disponível em: https://www.ecdc.europa.eu/sites/default/files/documents/Overview-rapid-test-situation-for-COVID-19-diagnosis-EU-EEA.pdf
5. Presidente da CNPD. Audição da Presidente da Comissão Nacional de Proteção de Dados [Internet]. Portugal: Canal Parlamento; 2021. Disponível em: https://canal.parlamento.pt/?cid=5084&title=audicao-da-presidente-da-comissao-nacional-de-protecao-de-dados
6. Presidência do Conselho de Ministros. Decreto n.o 8/2020 de 8 de novembro. Diário da República, 1a série, No 217-A. 2020; 2–8.
7. CNPD. Orientações sobre os tratamentos de dados pessoais de saúde regulados no Decreto n.o 8/2020, de 8 de novembro. Vol. 2020. LISBOA; 2020.
8. Comissão Nacional de Protecão de Dados. Deliberação no 2021 /548. LISBOA; 2021.

O Papel do Encarregado de Proteção de Dados junto da Comissão de Ética para a Saúde

Fernanda Fragoso
DPO
SCML

O Regulamento Geral sobre a Proteção de Dados – RGPD elenca, no artigo 39º, as funções do Encarregado da Proteção de Dados – EPD, complementadas, no ordenamento jurídico nacional, pelo artigo 11º da Lei nº 58/2019, de 8 de agosto – Lei de execução do RGPD.

Genericamente, ambos os normativos atribuem ao EPD funções de aconselhamento junto do responsável pelo tratamento, ou do subcontratante, e dos trabalhadores – entendendo-se lato sensu como todos os colaboradores daquela organização – bem como funções de controlo da conformidade com o RGPD, materializadas na repartição de responsabilidades, na sensibilização dos utilizadores, formação do pessoal e realização das auditorias correspondentes.

No n.º 2 do artigo 39º do RGPD, evidencia-se o quanto é importante o envolvimento do EPD em todas as questões relacionadas com a proteção de dados pessoais, dispondo que

"No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento."

O quadro legal da Investigação Clínica, aprovado pela Lei nº 21/2014, de 16 de abril, alterada pela Lei nº 73/2015, de 27 de julho, e pela Lei nº 49/2018, de 14 de agosto, define-a, no artigo 1º, nº1, *"como todo o estudo sistemático destinado a descobrir ou a verificar a distribuição ou o efeito de fatores de saúde, de estados ou resultados em saúde, de processos de saúde ou de doença, do desempenho e, ou, segurança de intervenções ou da prestação de cuidados de saúde."*

No artigo 1º, n.º 3, da citada lei verifica-se, desde logo, a relevância na articulação com a legislação relativa à proteção de dados pessoais – a então Lei nº 67/98, de 26 de outubro, revogada pelo artigo 66º da Lei nº 58/2019, de 8 de agosto – dando-lhe toda a prevalência no que à proteção de dados pessoais respeitasse.

No artigo 2º, a Lei da Investigação Clínica contempla, designadamente, as definições das Comissões de Ética para a Investigação Clínica (CEIC) e das Comissões de Ética para a Saúde (CES) e demonstra, claramente, a importância do consentimento informado, cuja definição, na alínea l), elenca os atributos inerentes ao consentimento da pessoa que vai participar no estudo clínico, exigindo que o mesmo seja prestado de forma expressa, livre e informada, por quem tenha capacidade para o prestar. Essa informação tem de abranger *"a natureza, o alcance, as consequências e os riscos do estudo"* e permitir que o participante no estudo retire o seu consentimento, sem consequências para o efeito.

O consentimento informado é o elo de ligação, por excelência, entre a matéria respeitante à investigação clínica e a matéria da proteção de dados pessoais, tratada no RGPD e na Lei nº 58/2019, de 8 de agosto.

Não descurando, obviamente, todas as questões respeitantes à segurança do tratamento que garantam a utilização das medidas técnicas e organizacionais que permitam minimizar ou mitigar o risco associado ao tratamento dos dados pessoais de categorias especiais, assegurando, designadamente, a confidencialidade, a integridade e a disponibilidade dos dados pessoais, **é no consentimento informado que melhor se traduz a preocupação com o princípio da dignidade da pessoa humana, em toda a sua plenitude!**

Desde sempre, o regime jurídico específico da investigação clínica teve a preocupação de assegurar a liberdade do consentimento do participante na investigação, no respeito pela sua autodeterminação.

Na já citada lei, importa, ainda, transcrever o disposto no artigo 3º, com a epígrafe **"Primado da pessoa humana":**

"1 - Os estudos clínicos são realizados no estrito respeito pelo princípio da dignidade da pessoa humana e dos seus direitos fundamentais.

2 - Os direitos dos participantes nos estudos clínicos prevalecem sempre sobre os interesses da ciência e da sociedade.

3 - Na realização dos estudos clínicos, devem ser tomadas todas as precauções no sentido do respeito da privacidade do indivíduo e da minimização de eventuais danos para os seus direitos de personalidade e para a sua integridade física e mental."

De entre as funções do EPD, o controlo da conformidade com o RGPD configura-se na necessidade de verificação permanente das operações de tratamento dos dados pessoais, procurando assegurar que as mesmas respeitam a dignidade do titular dos dados, tendo em conta a natureza, o âmbito, o contexto e as finalidades prosseguidas, conformes aos princípios enunciados no artigo 5º, do RGPD, a saber: princípios da lealdade, licitude e transparência; princípio da limitação das finalidades; prin-

cípio da minimização dos dados; princípio da exatidão; princípio da conservação; princípios da integridade e da confidencialidade e princípio da responsabilidade.

Na investigação clínica, onde a base de licitude para o tratamento dos dados pessoais é o consentimento do seu titular, é necessário aferir, caso a caso, se os atributos do consentimento estão conformes com o RGPD, concretamente o plasmado no artigo 4º, 11. Nesta análise, terá de se ter em conta o artigo 7º, n.º 4, e Considerandos 33, 42 e 43, o artigo 9º, nº 2, alínea j), o artigo 89º, nº 1, e os Considerandos 156, 159, 161.

O consentimento só pode constituir uma base de licitude válida se o titular dos dados tiver o controlo sobre a sua vontade, manifestada de forma livre, específica, informada e inequívoca!

Em conformidade com o acima referido, entende-se que o papel do EPD junto da CES terá, necessariamente, natureza consultiva, de complementaridade direcionada para as questões de privacidade e proteção de dados pessoais, ao abrigo do RGPD e da Lei de Execução, procurando certificar-se que foi dada a devida informação ao participante na investigação, através de uma linguagem clara e compreendida pelo mesmo, indicando-lhe os eventuais riscos.

Caso o tratamento dos dados pessoais pretenda servir finalidades múltiplas, elas terão de ser devidamente elencadas, uma vez que a granularidade do consentimento está intimamente ligada à separação das finalidades e respetivos consentimentos. Só assim é possível assegurar a liberdade daquela manifestação de vontade específica para determinado objetivo!

Nas Orientações do Comité Europeu para a Proteção de Dados – ainda enquanto Grupo de Trabalho do Artigo 29º, no documento WP 259, com a última redação revista e adotada em 10 de abril de 2018 – sobre o consentimento, na aceção do Regulamento (EU) 2016/679, é referido que para a obtenção de um consentimento válido há que fornecer ao titular dos dados a seguinte informação:

- A identidade do responsável pelo tratamento;
- O tipo de dados que serão recolhidos e utilizados;
- A finalidade de cada uma das operações de tratamento para que se solicita o consentimento;
- O direito de retirar, a todo o tempo, o consentimento;
- A informação sobre a utilização dos dados pessoais para a tomada de decisões automatizadas, de acordo com o artigo 22º, nº 2, alínea c), do RGPD; e
- Os possíveis riscos de transferência de dados para países terceiros, caso se verifique.

Caberá ao EPD, se o seu contributo for solicitado pela CES, a verificação de que toda a informação acima referida foi devidamente transmitida ao titular dos dados pessoais, possibilitando-lhe uma manifestação de vontade conforme ao regime da proteção de dados pessoais!

Videovigilância: o artigo 19º da Lei n.º 58/2019 e quais os locais onde não se podem colocar câmaras

Jorge Martinez Batalha
Fundador da Protec Dados
Consultor-Formador
Encarregado da Proteção de Dados (DPO)
Presidente do Conselho Fiscal da APDPO Portugal
LinkedIn

Desde que o Regulamento Geral sobre a Proteção de Dados (RGPD) começou a ser aplicável, em 25 de maio de 2018, deixou de ser necessário realizar qualquer notificação ou pedido de autorização, perante a Comissão Nacional de Proteção de dados (CNPD), para efeitos de instalação, ampliação ou renovação de sistemas de videovigilância. Na verdade, passou assim a ser o responsável pelo tratamento a ter de analisar, previamente, se o tratamento de dados pessoais, decorrente da utilização de um sistema de videovigilância, cumpre os requisitos do RGPD e da legislação nacional que seja aplicável.

Com a entrada em vigor da Lei n.º 58/2019, que assegura a execução, na ordem jurídica interna, do RGPD, ficou estabelecido, no artigo 19.º, onde é que não são admissíveis as câmaras de videovigilância, com finalidade de proteção de pessoas e bens. Mas será que ficou claro, explícito e inequívoco, para as organizações/empresas, os locais onde não se podem colocar câmaras?

Efetivamente, o artigo 19.º da Lei n.º 58/2019, refere, no n.º 2, que as câmaras não podem incidir sobre:

"a) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, 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 zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso" [negrito nosso].

Ainda no n.º 3 do referido artigo, é definido que, "nos estabelecimentos de ensino, as câmaras de videovigilância só podem incidir sobre os perímetros externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática".

Como vimos, o advérbio "designadamente" surge na alínea c) e na alínea d) do n.º 2 do artigo 19.º da Lei n.º 58/2019. Mas poderá a palavra "designadamente" vir suscitar dúvidas quanto aos locais onde as câmaras não podem incidir?

Num Acórdão do Supremo Tribunal Administrativo, ficou claro que o advérbio "designadamente" deve ter "um sentido especificativo e indicativo com que se pretende particularizar algo ou alguém, de entre uma série de elementos indiscriminados de um conjunto". É também este sentido que parece ser o mais adequado para a interpretação do 19.º artigo da Lei n.º 58/2019. Ou seja, muito para além dos exemplos particularizados, existem vários outros locais onde câmaras não podem incidir.

A este propósito, poder-se-á questionar se, por exemplo, é admissível a colocação de câmaras a incidir sobre o interior de uma igreja ou de um outro local de culto? Ou de locais destinados ao entretenimento de crianças (p.e. *play centers*)? Ou no interior de elevadores? Ou as câmaras poderão incidir sobre piscinas e imediações? Ou até no interior de bares ou restaurantes?

No artigo 19.º da Lei n.º 58/2019, as zonas de refeição reservadas a trabalhadores são expressamente identificadas como locais onde as câmaras não podem incidir. Mas não terá o cidadão comum, em todo o caso, o mesmo direito à privacidade durante a refeição no interior de um qualquer restaurante ou esplanada?

Na verdade, quando um titular dos dados entenda fazê-lo, tem o direito de apresentar uma queixa à autoridade de controlo. Para a finalidade de participações em matérias que envolvem videovigilância, sendo a CNPD a autoridade de controlo nacional para efeitos do RGPD e da Lei n.º 58/2019, decidiu adotar, parcialmente, o texto do 19.º artigo da Lei n.º 58/2019.

No formulário específico para efeitos de queixa sobre videovigilância, o cidadão que pretenda proceder a uma participação através do sítio da CNPD na Internet, encontra, numa das fases do processo de submissão, um conjunto de opções de escolha/preenchimento obrigatórios. Aqui, apesar de não estar incluída a categoria de titulares dos dados "**utentes**", ignorando

parcialmente a alínea c) do artigo 19.º da Lei n.º 58/2019, o advérbio "designadamente" surge, em duas opções, para efeito de participação, da mesma forma e quantidade que no texto do artigo 19.º da Lei n.º 58/2019. Parece ter existido intenção em manter inalterada a palavra em apreço. No entanto, não parece que esse facto seja vantajoso, para os titulares dos dados, quanto ao esclarecimento sobre os locais onde as câmaras não podem incidir.

É certo que no sítio da CNPD na Internet, num separador específico para esclarecimentos das organizações sobre videovigilância, aponta outros exemplos de locais onde não podem ser colocadas câmaras, para além do que é referido no 19.º artigo da Lei n.º 58/2019. No entanto, nada é indicado, por exemplo, quanto ao interior de um local de culto.

Neste âmbito, porque estão em causa dados que podem revelar convicções religiosas, incluídos nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, poderia ser seguido o limite definido, por exemplo, na autorização n.º 5824/ 2018, da CNPD, de 1 de maio de 2018, ainda antes da data em que começou a ser aplicável o RGPD (25 de maio de 2018), onde foi estabelecido que o responsável é autorizado a proceder ao tratamento de dados pessoais efetuado no âmbito da videovigilância, não podendo, "em circunstância alguma, serem recolhidas imagens no interior do local de culto".

Entende-se ser necessário clarificar que não podem ser recolhidas imagens de videovigilância no interior de um local de culto, mesmo que não exista gravação, ou seja, com visualização em tempo real. Isto porque, tal como já referiu o Comité Europeu para a Proteção de Dados, nas Diretrizes 3/2019, adotadas em 29 de janeiro de 2020, sobre tratamento de dados pessoais através de dispositivos de vídeo, "por vezes, o controlo em tempo real também pode ser mais intrusivo do que a conservação e a eliminação automática do material após um período de tempo limitado (por exemplo, se alguém estiver constantemente a visualizar o monitor, o método pode ser mais intrusivo do que se não houver nenhum monitor e o material for diretamente armazenado numa caixa negra)".

Outro âmbito que deve ter particular atenção é aquele que envolva crianças. À condição de vulnerabilidade das crianças, deveria corresponder uma maior proteção dos seus dados, até porque o RGPD, no Considerando (38), refere que "as crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais". Também nessa linha de pensamento, antes do RGPD ser aplicável, os locais destinados ao entretenimento de crianças já eram alvo de estabelecimento de limites pela CNPD. Veja-se o exemplo da autorização n.º 12829/2016, onde, para efeitos de um tratamento de dados pessoais resultante de videovigilância, com a finalidade de proteção de pessoas e bens, era estabelecido que "na eventualidade de existir um local destinado ao entretenimen-

to de crianças (p.e. *play centers*), não podem ser recolhidas imagens desse espaço". No entanto, à data em que é escrito este artigo, não se conhece nenhuma orientação da CNPD sobre esta matéria.

Contudo, os sistemas de videovigilância continuam a ser instalados. Por isso, deve também ser tido em conta que as entidades que procedem à conceção, instalação, manutenção e assistência técnica de sistemas de videovigilância (vulgarmente referidos como instaladores de sistemas de segurança), têm dificuldade em identificar, de modo inequívoco, quais os locais onde não devem incidir as câmaras. Assim, encontram-se limitados na prestação de esclarecimentos ao responsável pelo tratamento resultante de videovigilância, com a finalidade de proteção de pessoas e bens, quanto à necessidade de salvaguardar a privacidade desde a conceção e por defeito, tal como referido no artigo 25.º do RGPD. Existe, por isso, um risco de incumprimento por parte destas entidades, na sua condição de subcontratante, para além do próprio responsável, para efeitos do disposto no RGPD, da Lei n.º 58/2019 e demais legislação aplicável.

Em suma, parece evidente a necessidade de um esclarecimento adicional por parte da CNPD, para que se torne claro, explícito e inequívoco, para as organizações/empresas, os locais onde não se podem colocar câmaras.

Tal como o fez em tempos, em matéria de videovigilância, na sua Deliberação n.º 61/2004, de 19 de abril, a CNPD deveria agora clarificar, entre outros aspetos, o que deve ser entendido por "interior de área reservada a clientes ou utentes onde deva ser respeitada a privacidade". Adicionalmente, clarificar o que deva ser entendido por "interior de área reservada a trabalhadores".

Além disso, no formulário específico para efeitos de queixa sobre videovigilância, da CNPD, parece ser necessário criar um espaço de texto livre, para o queixoso indicar o local que entende ser uma área reservada a clientes ou utentes onde deva ser respeitada a privacidade ou, também, o local exato do interior de área reservada a trabalhadores.

Por fim, sendo a CNPD a autoridade de controlo nacional para efeitos do RGPD e da Lei n.º 58/2019, espera-se que, tal como refere o Considerando (132) do RGPD, antes das medidas sancionatórias, as atividades de sensibilização das autoridades de controlo dirigidas ao público devam incluir medidas específicas a favor dos responsáveis pelo tratamento e subcontratantes.