O encarregado de proteção de dados

Data protection officer

10.29073/j2.v8i1.1120

Recebido: 08 de março de 2026.
Aprovado: 31 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Sílvia Cardoso, ESTG-IPP, Portugal, silviacardosolg@gmail.com.

Resumo

O presente artigo analisa a figura jurídica do Encarregado de Proteção de Dados (EPD), prevista no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, designado por Regulamento Geral sobre a Proteção de Dados (RGPD), e concretizada no ordenamento jurídico português pela Lei n.º 58/2019, de 8 de agosto (LE).

O estudo incide sobre o enquadramento jurídico do EPD, abordando o seu conceito, características, formação e posição na organização. Analisa-se igualmente o regime de designação desta figura, com particular enfoque nas entidades públicas, bem como as funções e obrigações que lhe são atribuídas pela legislação europeia e nacional. Por fim, procede-se à análise das consequências jurídicas associadas ao incumprimento das normas de proteção de dados e à eventual responsabilidade decorrente da atuação do EPD.

O trabalho baseia-se numa metodologia jurídico-dogmática, assente na análise da legislação aplicável, bem como da doutrina e orientações relevantes em matéria de proteção de dados.

Palavras-Chave: Administração Pública; Compliance; Encarregado de Proteção de Dados; Proteção de Dados; RGPD.

Abstract

This article analyzes the legal figure of the Data Protection Officer (DPO), established by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, commonly known as the General Data Protection Regulation (GDPR), and implemented in the Portuguese legal system through Law No. 58/2019 of 8 August (EL).

The study examines the legal framework of the DPO, addressing its concept, characteristics, professional qualifications and position within organizations. It further analyzes the designation regime of the DPO, with particular emphasis on public entities, as well as the functions and obligations assigned to this role under European and national legislation. Finally, the article discusses the legal consequences associated with non-compliance with data protection rules and the potential liability arising from the actions of the DPO.

The research follows a legal-dogmatic methodology based on the analysis of applicable legislation, doctrinal contributions and relevant guidelines in the field of data protection.

Keywords: Compliance; Data Protection; Data Protection Officer; GDPR; Public Administration.

1. Introdução

A crescente digitalização da sociedade e o desenvolvimento das tecnologias de informação conduziram a um aumento significativo da recolha e tratamento de dados pessoais por organizações públicas e privadas. Neste contexto, a proteção de dados pessoais assumiu particular relevância no ordenamento jurídico europeu, culminando na aprovação do Regulamento (UE) 2016/679, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD).

O RGPD estabeleceu um quadro jurídico harmonizado em matéria de proteção de dados na União Europeia, introduzindo novos mecanismos destinados a reforçar a proteção dos direitos fundamentais dos titulares dos dados e a garantir maior responsabilização das organizações no tratamento de dados pessoais

Entre esses mecanismos destaca-se a figura do Encarregado de Proteção de Dados (EPD), cuja função consiste em assegurar o acompanhamento do cumprimento das normas relativas ao tratamento de dados pessoais, bem como promover a cultura de proteção de dados no seio das organizações (Cordeiro, 2021; Grupo de Trabalho do Artigo 29º, 2017).

Embora o RGPD preveja expressamente a existência e as funções do EPD, a sua concretização nos ordenamentos jurídicos nacionais exige a articulação com legislação interna. Em Portugal, essa concretização ocorreu através da Lei n.º 58/2019, de 8 de agosto (LE), que assegura a execução do RGPD e estabelece normas complementares relativas à sua aplicação no ordenamento jurídico nacional.

O presente artigo tem como objetivo analisar o regime jurídico aplicável ao Encarregado de Proteção de Dados no contexto do ordenamento jurídico português, incidindo sobre o seu enquadramento legal, as suas funções e obrigações, bem como sobre os desafios associados à sua posição nas organizações.

A investigação baseia-se numa metodologia jurídico-dogmática, assente na análise da legislação europeia e nacional aplicável, complementada pela análise de orientações doutrinárias e institucionais relevantes.

2. Enquadramento Legal

2.1. Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD foi aprovado em 27 de abril de 2016 pelo Parlamento Europeu e pelo Conselho, tendo como objetivo reforçar a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e assegurar a livre circulação desses dados no espaço da União Europeia.

Este regulamento entrou em vigor no vigésimo dia após a sua publicação no Jornal Oficial da União Europeia, tornando-se aplicável a partir de 25 de maio de 2018, revogando a Diretiva 95/46/CE, que até então constituía o principal instrumento jurídico europeu nesta matéria.

Apesar do RGPD ser diretamente aplicável em todo o território da União Europeia (UE) desde 25 de maio de 2018, a verdade é que o mesmo permite aos Estados Membros (EM), a manutenção ou aprovação de disposições específicas no que concerne à aplicação de determinadas regras respeitantes ao tratamento de dados.

De acordo com o art.º 1º do RGPD, o objeto do RGPD consiste em regular a "*proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*.", alcançando assim dois grandes objetivos, defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados e, ainda, promover a livre circulação dos dados pessoais.

Entre os mecanismos previstos pelo regulamento, destaca-se no seu âmbito, a figura jurídica do Encarregado de Proteção de Dados (EPD), consagrada nos artigos 37º a 39º do RGPD, figura esta existente já em vários países antes da entrada em vigor do RGPD.

2.2. Lei de Execução do RGPD em Portugal – Lei n.º 58/2019, de 08 de Agosto (LE)

Assim, para a aplicação do Regulamento Geral de Proteção de Dados em Portugal, foi publicado no Diário da República, 2.ª série – N.º 163, o Despacho n.º 7456/2017, de 24 de agosto, que criou um Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação daquele regulamento, tendo este Grupo apresentado uma proposta de lei ao Governo, aprovada em Conselho de Ministros e remetida à Assembleia da República.

Ora, desta proposta surgiu a Lei n.º 58/2019, de 08 de agosto (Lei de execução interna do RGPD (LE)), que veio assegurar a execução do RGPD, no ordenamento jurídico português, após um longo processo legislativo.

Além de assegurar a execução do RGPD na ordem jurídica portuguesa, esta lei visou ainda harmonizar a legislação nacional e aprofundar a regulação da proteção de dados em diferentes matérias e mais detalhadamente.

Deste modo, a LE estatuiu no seu Capítulo III, designadamente os artigos 9º a 13º, as normas aplicáveis ao Encarregado de Proteção de Dados (EPD).

Destaca-se que, relativamente a esta LE, a Comissão Nacional de Proteção de Dados (CNPD) decidiu, menos de um mês após a sua entrada em vigor, desaplicar algumas normas do referido diploma legal em situações de tratamento de dados pessoais a serem avaliadas futuramente, através da Deliberação n.º 2019/494 (CNPD, 2019). Nesse documento, a CNPD, num texto extenso, formula críticas severas ao processo legislativo português que conduziu à aprovação desta LE, justificando a desaplicação de determinadas normas pelo facto de estas contrariarem o previsto no RGPD, comprometendo assim a sua aplicação uniforme e, consequentemente, a sua plena eficácia e consistência em todo o território dos Estados-Membros.

3. O Encarregado de Proteção de Dados

Apesar da relevância desta figura no sistema de proteção de dados, o artigo 4º do RGPD não contém uma definição expressa de Encarregado de Proteção de Dados. Ainda assim, o regulamento estabelece o regime jurídico aplicável a esta figura nos artigos 37º a 39º, permitindo identificar as suas características essenciais.

Assim, por interpretação extensiva do RGPD, o EPD pode ser entendido como a pessoa singular ou coletiva designada por uma organização para acompanhar e monitorizar o cumprimento das normas relativas à proteção de dados pessoais (Portal DPO). A sua atuação envolve a participação em todas as questões relacionadas com o tratamento de dados pessoais, desempenhando um papel central na implementação das políticas de proteção de dados no seio da organização (Cordeiro, 2021).

No exercício das suas funções, o EPD encontra-se sujeito a um dever de sigilo e confidencialidade relativamente às informações a que tenha acesso no âmbito da sua atividade. Este dever abrange todas as informações a que tenha tido acesso durante esse exercício, tanto as informações relativas ao responsável pelo tratamento como aquelas respeitantes aos titulares dos dados, mantendo-se mesmo após o termo das funções que lhe deram origem, nos termos do artigo 10º da LE.

Deste modo, o Encarregado de Proteção de Dados assume um papel fundamental no sistema de gestão da proteção de dados, atuando como elemento de ligação entre a organização, os titulares dos dados e a autoridade de controlo.

3.1. Características, Formação e Posição

Independentemente da natureza da relação jurídica que mantém com a organização, o encarregado de proteção de dados deve exercer as suas funções com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante, nos termos do n.º 2, do artigo 9.º da LE.

Relativamente à autonomia técnica do EPD, destaca-se o Considerando 97 do RGPD,

Que estabelece que "*O nível necessário de conhecimentos especializados deverá ser*

determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante" e ainda que os "*encarregados de proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência*".

Este dispositivo evidencia que a função do EPD nem sempre é fácil ou conciliável quando desempenhada por um trabalhador da organização subordinado juridicamente por um contrato individual de trabalho, acumulando simultaneamente duas funções muito distintas: a de funcionário subordinado, sujeito ao poder diretivo e disciplinar da organização, e a de EPD, responsável por fiscalizar a atuação da própria organização, sem receber

ordens de superiores hierárquicos e sem poder ser penalizado ou destituído das suas funções (n.º 3 do artigo 38º do RGPD).

Assim, a organização deve realizar uma análise baseada no risco para avaliar se a designação de um EPD interno é adequada. Caso identifique conflitos de interesse ou risco elevado, poderá optar pela designação de um EPD externo, que exerça as funções em regime de exclusividade, mediante contratação de prestação de serviços através de procedimento de contratação pública, minimizando os riscos para a organização.

Ademais, este EPD tem um dever de lealdade para com a organização, bem como um dever de cooperação com a Comissão Nacional da Proteção de Dados (CNPD), designadamente informando esta entidade fiscalizadora de eventuais incumprimentos da lei pela organização, o que poderá causar um conflito de deveres do EPD. Neste sentido, conforme se referiu anteriormente, a melhor solução será a contratação de consultor externo para o exercício das funções de EPD.

A independência funcional do EPD constitui um requisito fundamental para garantir a eficácia da sua atuação. Sempre que acumula funções de EPD com outras responsabilidades na organização, deve ser garantida uma segregação adequada de funções, de modo a prevenir conflitos de interesse. Segundo o Grupo de Trabalho do Artigo 29º para a proteção de dados (GT 29), o EPD não deve ocupar uma posição na organização em que tenha autoridade para decidir sobre as finalidades e os meios de tratamento de dados. O GT 29 apresenta ainda diversas boas práticas destinadas à prevenção de conflitos de interesse no exercício desta função.

No que respeita à formação do EPD, embora não seja exigida qualquer certificação profissional, o n.º 5 do artigo 37º do RGPD estabelece que "*O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.*".

Assim, dada a importância atribuída a tal cargo, especialmente na Administração Pública, o critério de nomeação do EPD deve ser rigoroso. O EPD deve possuir conhecimentos sólidos, adequados e específicos em matéria de proteção de dados e procedimentos administrativos do organismo, formação jurídica na área do direito e, ainda, competências na área dos sistemas de informação, de modo a garantir o desempenho eficaz das funções previstas no artigo 39º. A ausência dessas competências essenciais pode comprometer a conformidade legal da organização, expondo-a ao risco de infrações e à aplicação de coimas.

Neste contexto, a designação do EPD deve considerar a sua experiência e formação específica, bem como a natureza das atividades desenvolvidas na organização. O nível de competências exigido e o grau de apoio disponibilizado devem ser proporcionais à complexidade das operações de tratamento de dados e à quantidade de dados sensíveis processados pela organização.

Nos termos do artigo 38º do RGPD, o EPD deve ser envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais, que sejam tratadas pelo responsável pelo tratamento e o subcontratante, devendo estes apoiar o EPD no exercício das suas funções, fornecendo-lhe os recursos necessários ao seu desempenho e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

O EPD deve ser isento e imparcial no exercício das suas funções e deve informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

Os titulares dos dados podem contactar o encarregado da proteção de dados sobre

todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos seus direitos.

Ora, a imposição obrigatória deste EPD tem como propósito uma função especializada no controlo relativamente ao *compliance* de proteção de dados. O termo *compliance* refere-se ao "*conjunto de ações ou procedimentos que visam verificar o cumprimento de leis, regulamentos, normas ou padrões estabelecidos, geralmente numa*

empresa ou instituição; verificação da conformidade (Dicionário Priberam da Língua Portuguesa online (s.d.), Contudo, a responsabilidade principal por esse controlo recai sobre a própria organização, cabendo ao EPD atuar como uma segunda linha de defesa, complementar à supervisão da autoridade de controlo e, simultaneamente, como provedor dos titulares dos dados (Cordeiro, 2021).

O EPD encontra-se subjugado ao dever de sigilo ou de confidencialidade no exercício

das suas funções, podendo exercer outras funções e atribuições, desde que estas não resultem num conflito de interesses.

A título informativo, foi criado pelo consultor Tiago Nascimento um projeto de implementação do RGPD denominado "*Portal do DPO*", um portal que permite o acesso a conceitos e informações essenciais para assegurar a conformidade das organizações com o regulamento. Este recurso foi criado em resposta às frequentes dúvidas e incertezas sobre a interpretação do RGPD, configurando-se como uma ferramenta de trabalho que reúne direitos, deveres e boas práticas relacionados com o regulamento, podendo ser esclarecidas ainda dúvidas através do grupo de rede social *LinkedIn* (Pedreira, 2019).

3.2. Designação

Conforme já referido anteriormente, apesar desta figura ser uma novidade do RGPD, o seu conceito já existia antes, sendo que apenas agora se torna legalmente obrigatória a sua designação, verificadas determinadas condições constantes do n.º 1 do artigo 37º do RGPD.

O RGPD determina a obrigatoriedade de designar um EPD apenas nos seguintes casos expressamente previstos no artigo 37º do RGPD:

a) Quando o tratamento é efetuado por uma autoridade ou um organismo público, com exceção dos tribunais, desde que, no exercício da sua função jurisdicional, podendo ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

Esta exceção deve-se ao princípio constitucional da independência dos tribunais e consequente falta de competência das autoridades de controlo relativamente àqueles, conforme n.º 3 do art.º 55º do RGPD. Em referência à LE, esta substitui no seu n.º 1 do art.º 12º, o vocabulário usado pelo RGPD, aplicando o conceito de entidade pública e descrevendo no seu n.º 2 o que se deve compreender por entidade pública.

b) Nas empresas privadas quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala.

Estas presunções (atividades principais; controlo regular e sistemático e em grande

escala) apresentam algumas dificuldades uma vez que se baseiam em conceitos imprecisos e pouco concretizáveis (Cordeiro, 2021).

Esta norma determina os casos em que existe obrigatoriedade de designação de EPD

no setor privado, relevando-se aqui novamente o Considerando 97 quanto a esta matéria, pois resulta da sua leitura que as atividades principais dizem respeito às atividades primárias, sendo que quanto a estas atividades as orientações do GT 29 refere que as atividades principais podem entender-se como as operações essenciais necessárias para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, no entanto, esta interpretação não deve excluir as atividades em que o tratamento de dados constitui uma parte indissociável das atividades do responsável pelo tratamento ou do subcontratante.

Quanto ao controlo, de acordo com o GT 29, este compreende a observação do comportamento do titular dos dados, comportamento este definido no Considerando 24 do RGPD, significando que o controlo regular é

permanente ou repetido periodicamente e o controlo sistemático ocorre de forma metódica, como parte de uma estratégia, de forma planeada e organizada, e como parte de um plano universal de recolha de dados pessoais. Relativamente à presunção de grande escala faz-se referência ao Considerando 91, em que se entende que as operações de tratamento de dados que digam respeito a uma grande quantidade de dados podem afetar um número considerável de titulares, resultando num risco elevado, pelo que o GT 29 recomenda que devam ser considerados certos fatores para determinar se o tratamento é efetuado em grande escala, tais como, o número de titulares de dados, a quantidade e a diversidade de tipos de dados, a duração ou permanência das atividades de tratamento de dados e a extensão geográfica da atividade de tratamento.

c) Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (art.º 9º) ou de dados pessoais relacionados com condenações penais e infrações (art.º 10º). Esta designação está relacionada com a natureza sensível destes dados, obtendo assim uma proteção acrescida.

Refere ainda este artigo que um grupo empresarial (grupo composto pela empresa que exerce o controlo e pelas empresas controladas (Considerando 37 e definição 19 do artigo 4º do RGPD), poderá também designar um único encarregado de proteção de dados desde que haja um encarregado de proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

E ainda, quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou organismo público, pode ser designado um único EPD para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

É de salientar a designação voluntária do n.º 4 em que, no caso do responsável pelo tratamento de uma empresa opte, ainda que não seja obrigatório, por designar um EPD, fica desde logo obrigado ao cumprimento de todas as obrigações subjacentes como se se tratasse de uma designação obrigatória (Universidade de Coimbra, s.d.).

Quando é designado um EPD pelas organizações, é obrigatória a publicação dos seus contactos, bem como existe o dever de informação pelo responsável de tratamento e o dever de comunicação sobre o EPD à autoridade de controlo (CNPD).

No que concerne à LE, esta apenas vem complementar o disposto no RGPD, no que respeita a critérios de designação do EPD e à autonomia técnica do mesmo, temas estes já abordados no ponto 1.3.

3.2.1. Designação em Autoridades ou Organismos Públicos

As entidades públicas estão sempre obrigadas a ter um EPD, encontrando-se essa regulação mais concretamente no artigoº 12º da LE, dispondo o n.º 2 sobre quais as entidades que são consideradas públicas.

O n.º 3 impõe a existência de pelo menos um EPD e qual o respetivo responsável de tratamento em cada uma das entidades, a saber:

a) Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respetivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;

b) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respetivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;

c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;

d) Nas freguesias em que tal se justifique, nomeadamente naquelas com mais de 750 habitantes, sendo designado pela junta de freguesia, com faculdade de delegação no presidente.

No que respeita à exigência quantitativa (750 habitantes) referida nesta alínea, a mesma não pode ser aplicada, uma vez que a legislação nacional não se pode sobrepor à obrigação imposta pelo RGPD na sua alínea a) do n.º

1 do art.º 37º, i.é., a mera designação de um EPD sempre que o tratamento for efetuado por uma autoridade ou um organismo público;

e) Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação no respetivo presidente.

Conforme se disse anteriormente, tendo em conta a respetiva estrutura organizacional e dimensão das autoridades ou organismos públicos, pode ainda ser designado um único EPD de acordo com o preceituado no n.º 4 deste artigo 12º, conjugado com o n.º 3 do artigo 37º do RGPD.

A designação do EPD cabe a cada entidade, não sendo obrigatório o exercício de funções em regime de exclusividade.

No entanto, O EPD de uma entidade pública que tenha atribuições de regulação ou controlo não pode exercer essas funções simultaneamente em entidade sujeita ao controlo, ou inserida no perímetro regulatório daquela entidade.

3.3. Funções e Obrigações

A função de EPD deve ser atribuída sempre que exista processamento de dados pessoais e sensíveis em larga escala, envolvendo o aconselhamento, a monitorização e conformidade de toda a segurança e proteção de dados.

O artigo 39º do RGPD estabelece para o EPD as seguintes funções/obrigações:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, sobre todas as questões relacionadas com a proteção de dados, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do regulamento e da LE;

b) Controlar a conformidade com o regulamento, com a LE e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

No que respeita à realização de auditorias, não se afigura que estas devam ser executadas diretamente pelo EPD. Nos termos da alínea a) do artigo 11º da LE, incumbe ao EPD garantir a existência de mecanismos de controlo do cumprimento das normas de proteção de dados, designadamente através da implementação de programas de auditorias independentes. Tal função não implica, contudo, que o próprio EPD seja responsável pela sua realização.

Com efeito, uma parte significativa do objeto dessas auditorias incide precisamente sobre o sistema de controlo da conformidade cuja monitorização compete ao próprio EPD. Se a realização das auditorias fosse assegurada diretamente pelo EPD, tal poderia configurar uma situação de autoverificação capaz de afetar a independência e a eficácia da função de monitorização que lhe está atribuída, criando um potencial conflito de interesses (Cordeiro, 2021).

De um modo geral, a auditoria interna em matéria de proteção de dados visa avaliar a conformidade das práticas organizacionais com os requisitos legais aplicáveis, bem como verificar a eficácia das ações implementadas na sequência de auditorias anteriores. Paralelamente, permite identificar aspetos organizacionais suscetíveis de melhoria, através da análise de evidências e da verificação da adequação e eficácia dos controlos existentes para a mitigação dos riscos associados ao tratamento de dados pessoais.

Nesse contexto, as auditorias possibilitam a identificação de situações de não conformidade e de oportunidades de melhoria que deverão ser posteriormente tratadas pela organização, contribuindo para o reforço contínuo do sistema de gestão da proteção de dados.

Assim, não se afigura adequado que a sua realização seja assegurada pelo próprio EPD, uma vez que tal poderia comprometer o efeito útil da atividade de monitorização que lhe está atribuída, ao colocar na mesma entidade a responsabilidade simultânea pela avaliação e pela supervisão do sistema de controlo do cumprimento.

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados, controlando a sua realização nos termos do artigo 35º;

d) Cooperar com a autoridade de controlo (CNPD);

e) Contactar a CNPD sobre questões relacionadas com o tratamento, incluindo a consulta prévia referida no art.º 36.º, bem como consultar a CNPD sobre qualquer outro assunto.

Em relação à LE as funções do EPD encontram-se estatuídas no artigo 11º, acrescentando este dispositivo legal três funções além das já elencadas no RGPD, designadamente:

a) Assegurar a realização de auditorias, quer periódicas, quer não programadas (ponto já desenvolvido anteriormente);

b) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;

Esta função é uma duplicação das funções já existentes nas alíneas a) e b) do artigo 39º do RGPD que preveem a informação, aconselhamento, sensibilização e formação dos trabalhadores;

c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela LE.

Também esta função em nada vem acrescentar às funções já estabelecidas no RGPD, pois que o n.º 4 do artigo 38º daquele regulamento incumbe ao EPD a função de ponto de contacto com os titulares dos dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais.

3.4. Incumprimento e Violação

O regime sancionatório aplicável às violações das normas de proteção de dados encontra-se previsto no Capítulo VIII do RGPD (artigos 77º a 84º), que regula as vias de recurso, a responsabilidade e as sanções.

No ordenamento jurídico português, a LE estabelece igualmente um regime contraordenacional aplicável às infrações em matéria de proteção de dados na Secção II do Capítulo VII (artigos 37º a 45º).

Importa salientar que as sanções previstas na legislação incidem essencialmente sobre o responsável pelo tratamento ou o subcontratante, não recaindo diretamente sobre o EPD.

Não obstante, em determinadas circunstâncias poderá existir responsabilidade, caso se verifique que a violação resultou de uma atuação negligente do EPD. Nessa hipótese, poderá assistir ao responsável pelo tratamento ou ao subcontratante o direito de regresso contra aquele, nos termos dos números 2 e 5 do artigo 82º do RGPD, bem como em conformidade com a parte final do Considerando 146 do mesmo diploma, segundo o qual: "…*Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento*.".

Ademais, nos termos do artigo 51º da LE, o EPD pode ser ainda responsável criminalmente no caso de violação do dever de sigilo profissional a que está obrigado nos termos da lei se, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais, sendo punido com pena de prisão até 2 anos ou com pena de multa até 240 dias, uma vez que estas penas são agravadas quando praticadas por EPD. Por outro lado, a negligência também é punível, embora de modo mais ligeiro, com pena de prisão até 6 meses ou com pena de multa até 60 dias.

4. Conclusão

Face ao exposto, conclui-se que, no atual quadro normativo de proteção de dados pessoais, o Encarregado de Proteção de Dados (EPD) assume um papel estruturante na concretização das obrigações decorrentes do Regulamento Geral sobre a Proteção de Dados (RGPD) e da legislação nacional aplicável. Esta figura jurídica configura-se como um elemento central no sistema de gestão da proteção de dados, na medida em que assegura a monitorização do cumprimento das normas legais e promove a implementação, no seio das organizações públicas e privadas, de mecanismos e procedimentos destinados a garantir a licitude, integridade, confidencialidade e segurança no tratamento de dados pessoais. Neste contexto, a designação de um EPD implica um elevado grau de responsabilidade e complexidade funcional, o que se reflete na exigência de qualificações técnicas especializadas, bem como de competências profissionais adequadas ao exercício destas funções.

No âmbito da presente análise foram igualmente consideradas potenciais situações de conflito de interesses à designação de um EPD enquanto trabalhador da própria organização. Tal problemática revela particular relevância quando o titular desta função se encontra simultaneamente sujeito ao poder diretivo e disciplinar da entidade e incumbido de fiscalizar a conformidade das suas práticas com o regime jurídico aplicável, devendo, nos termos do RGPD, exercer as suas funções com autonomia e independência, sem receber instruções quanto ao desempenho das mesmas e sem sofrer qualquer tipo de penalização ou destituição em razão da sua atuação. Neste sentido, entende-se que as organizações deverão proceder a uma avaliação prévia baseada no risco, com vista a determinar a adequação da designação de um EPD interno. Caso se conclua pela existência de constrangimentos suscetíveis de comprometer a independência funcional exigida, a designação de um EPD externo poderá constituir uma solução adequada, permitindo assegurar o pleno exercício das suas atribuições, nomeadamente no que respeita à cooperação com a CNPD.

Foram também ponderadas eventuais tensões decorrentes da atribuição ao EPD da responsabilidade de assegurar a realização de auditorias ao sistema de proteção de dados. Considerando que compete ao EPD monitorizar o cumprimento das normas aplicáveis, a sua intervenção direta na execução dessas auditorias poderá comprometer a imparcialidade e a eficácia do sistema de controlo, recomendando-se, por conseguinte, a clara delimitação de funções no âmbito das estruturas de *compliance* organizacional.

Em termos conclusivos, pode sustentar-se que a conformidade das organizações com o RGPD, designadamente através da designação de um EPD e da efetiva valorização do seu papel na definição e implementação de medidas adequadas de proteção de dados, constitui um fator determinante para a consolidação de uma cultura organizacional orientada para a responsabilidade e a transparência no tratamento de dados pessoais. Tal realidade não só reforça o cumprimento das obrigações legais, como contribui igualmente para o fortalecimento da confiança institucional e da credibilidade das organizações perante titulares de dados, entidades reguladoras e a sociedade em geral.

Referências

Barreto Menezes Cordeiro, A. (2021). *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Edições Almedina.

Comissão Nacional de Proteção de Dados. (2019, setembro 3). *Deliberação/2019/494*. https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2019&type=2&ent=

Despacho n.º 7456/2017 (2017, agosto 24). *Diário da República, 2ª série, n.º 163*. https://dre.pt/dre/detalhe/despacho/7456-2017-108041501

Dicionário Priberam da Língua Portuguesa. (n.d.). *Compliance*. https://dicionario.priberam.org/compliance

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2016). *Orientações sobre os encarregados da proteção de dados (EPD) (WP243 rev.01)*. https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

Lei n.º 58/2019. (2019, agosto 8). *Diário da República, 1ª série, n.º 151*. https://dre.pt/dre/detalhe/lei/58-2019-123815982

Pedreira, F. (2019, novembro 5). Uma nova porta para os dados pessoais. *ECO*. https://eco.sapo.pt/2019/11/05/uma-nova-porta-para-os-dados-pessoais/

Parlamento Europeu & Conselho da União Europeia. (2016, abril 27). *Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, L 119. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679

Portal do DPO. (n.d.). *Glossário RGPD*. https://www.portaldodpo.pt/glossario/

Universidade de Coimbra. (n.d.). *Encarregado de Proteção de Dados*. https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/encarregado-protecao-dedados/

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.