DPO mag

EDIÇÃO Nº 11
JUL / 26

APDPO PORTUGAL

www.dpo-portugal.pt

DPO mag

EDIÇÃO Nº 11
JUL / 26

APDPO PORTUGAL

www.dpo-portugal.pt

DPO | magazine

FICHA TÉCNICA

NOME
DPO | magazine

PROPRIEDADE
APDPO Portugal – NIF 541502835

DIRETORA
Inês Oliveira

EDITOR
Luís Ferreira Mendes

PERIODICIDADE
Semestral

PREÇO
Gratuito

CONTACTO GERAL
geral@dpo-portugal.pt

UM PROJETO APDPO
ISSN 2184-8211

COPYRIGHT

DPO|magazine: a primeira revista do setor na Europa lançada a 28 de outubro de 2020.

Estatuto Editorial

A DPO|magazine é um projeto de informação internacional que visa preencher espaços vazios e acrescentar valor ao campo da proteção e segurança dos dados e da informação.
A DPO|magazine tem carácter digital, é independente e livre, sem interesses partidários ou económicos, e sem estabelecer hierarquias de funções ou de sectores de atividade, nas suas opções editoriais.
A DPO|magazine pauta-se por padrões de exigência na qualidade da informação e do conhecimento que veicula, primeiro garante da sua credibilidade e afirmação.
A DPO|magazine não fixa fronteiras geográficas, culturais ou temporais, recusando situações de sensacionalismo, exploração ou especulação.
A DPO|magazine fomenta o debate consciente e respeitável das grandes questões que se colocam às sociedades atuais, na perspetiva da melhoria do conhecimento.
A DPO|magazine é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e disponibilidade quotidianas para o estímulo à reflexão e ao conhecimento.

Conteúdo

O Conteúdo da DPO|magazine estará em permanente adaptação, procurando satisfazer a necessidade de melhor exposição dos temas que elegemos para entregar aos nossos leitores.

Presentemente a revista organiza-se em:

| Artigos
| Conteúdos de parceiros
| Debates
| Entrevistas
| Informações institucionais
| Opiniões
| Publicidade
| Reportagens

A QUEM SE DESTINA?

| Administradores e Gestores de Empresas
| Cargos dirigentes da Administração Pública
| Encarregados de Proteção de Dados
| Técnicos de Proteção de Dados
| Técnicos de Compliance
| Advogados, Solicitadores e Agentes de Execução
| Consultores e Auditores
| Economistas e Contabilistas
| Engenheiros informáticos e de Arquitetura de Sistemas
| Especialistas em Proteção e Segurança de Dados
| Especialistas em Segurança Informática e Cibersegurança
| Especialistas em Sistemas de Informação
| Especialistas em Transformação Digital
| Gestores e Analistas de Dados
| Profissionais BAD, da Informação e do Conhecimento
| Técnicos de Informação e Comunicação
| Técnicos de Recursos Humanos

PUBLICIDADE

Dispomos das seguintes opções para inserção de anúncios: | 2 páginas
| 1 página
| 1/2 página horizontal


APDPO
PORTUGAL

Mensagem da Diretora

Diretora da DPO Magazine

Bem-vindos à DPO Magazine n.º 11!

Na última edição da DPO Magazine, partilhei nesta mensagem inicial que as notícias nos traziam a novidade de que a Comissão Europeia se preparava para apresentar alterações ao Regulamento Geral sobre a Proteção de Dados (RGPD).

Tal cumpriu-se: a Comissão Europeia apresentou já uma proposta de Regulamento, que, entre outros, altera o RGPD.

Nas próximas linhas partilho aquelas que considero ser as 5 principais alterações, em tom crítico e não concordante. Vejamos.

1. Em primeiro lugar, propõe-se alterar o conceito de dados pessoais. À definição que Todos já conhecemos, é proposto aditar o seguinte:

«As informações relativas a uma pessoa singular não são necessariamente dados pessoais para qualquer outra pessoa ou entidade pelo simples facto de uma entidade poder identificar essa pessoa singular. As informações não são pessoais para uma determinada entidade se essa entidade não conseguir identificar a pessoa singular a quem dizem respeito, tendo em conta os meios que apresentem uma probabilidade razoável de ser utilizados por essa entidade. Essas informações não se tornam pessoais para essa entidade pelo simples facto de um potencial destinatário subsequente dispor de meios que apresentem uma probabilidade razoável de ser utilizados para identificar a pessoa singular a quem as informações dizem respeito.»

Criticando esta proposta de alteração, trago à colação duas ordens de razão que me motivam: por um lado, a nova proposta de definição deixa de ser focada no titular dos dados, passando a ser critério determinador do conceito de dados pessoais a entidade, em concreto *a probabilidade razoável de ser utilizados* [dados pessoais] *por essa entidade*.

Ora, o RGPD visa proteger os titulares dos dados, disso não há dúvidas; por isso mesmo, o conceito basilar de dados pessoais é desenhado em torno do titular, com foco nele e para sua proteção. Desfocar o conceito de dados pessoais e passar a ter uma definição cujo critério é a entidade que os trata obriga-nos à conclusão de que esta proposta desprotege o cidadão. Por isso mesmo, é contra ela que me posiciono.

Por outro lado, esta proposta torna o conceito de dados pessoais complexo e de verificação casuística, atividade de tratamento a atividade de tratamento, o que vai trazer mais burocracia às organizações e a perceção de que o RGPD só complica (ainda mais). A tal acrescenta-se o facto de hipotecar todo o regime aplicável à subcontratação, desvalorizando o que chama *potencial destinatário subsequente*. Deixem-me ser clara: tal como está, o conceito de dados pessoais mata a proteção conferida aos titulares de dados dada em sede de regime legal da subcontratação.

2. Em segundo lugar, ainda no artigo do RGPD dedicado às definições, propõe-se aditar, entre outras, a seguinte:

"Investigação científica", qualquer investigação que também possa apoiar a inovação, como o desenvolvimento tecnológico e a demonstração. Estas ações devem contribuir para os conhecimentos científicos existentes ou aplicar os conhecimentos existentes de formas inovadoras, ser realizadas com o objetivo de contribuir para o aumento dos conhecimentos gerais e do bem-estar da sociedade e respeitar os padrões éticos na área de investigação em causa. Tal não exclui a possibilidade de a investigação visar igualmente a promoção de um interesse comercial.»

Para criticar esta proposta, trago à colação o livro que estou a ler: Algoritmocracia - Como a IA está a Transformar as Nossas Democracias, de Adolfo Mesquita Nunes (cuja leitura a Todos recomendo, permitam-me a sugestão). Neste livro fica clarificado o rigor do método científico na busca da verdade, que muito se distancia dos interesses comercias das empresas do nosso tempo. Propor que o RGPD passe a equiparar uma investigação científica a qualquer inovação que promova um interesse comercial é perigoso para os direitos individuais e lesivo para o próprio conceito de democracia, que o citado livro densifica, nesta sociedade de vigilância em que vivemos.

3. Em terceiro lugar, esta proposta de alteração afasta o princípio da neutralidade tecnológica, ínsito no RGPD, passando a acolher expressamente os sistemas de IA e legitimando como base de licitude destes os interesses legítimos (cf. a proposta de alteração ao art. 9.º e a proposta de aditar um art. 88.º-C).

Com efeito, o RGPD, como princípio basilar, acolheu a neutralidade tecnológica – isto é, em nenhuma das suas normas alude expressamente a uma tecnologia. Fá-lo com o intuito de não ficar desatualizado a trecho breve, tanto quanto os desenvolvimentos tecnológicos. Regular expressamente uma tecnologia – a IA, note-se, revoga a neutralidade tecnológica e anula o seu efeito de perdurar nos tempos. Mas pior que tudo isso: a proposta legislativa cristaliza o interesse legítimo como base de licitude e fundamento de legitimidade para os tratamentos de dados no contexto do desenvolvimento e funcionamento de um sistema de IA, parecendo, em abstrato, assim fundamentá-los. Outra palavra não pode ser a de criticar.

4. Em quarto lugar, propõe-se alterar os deveres de informação, obrigação do responsável pelo tratamento, no seguinte sentido:

[…] *não são aplicáveis se os dados pessoais tiverem sido recolhidos no contexto de uma relação clara e circunscrita entre os titulares dos dados e um responsável pelo tratamento que exerça uma atividade que não implique a utilização intensiva de dados e se existirem motivos razoáveis para presumir que o titular dos dados já dispõe das informações a que se refere o n.º 1, alíneas a) e c), a menos que o responsável pelo tratamento transmita os dados a outros destinatários ou categorias de destinatários, transfira os dados para um país terceiro, tome decisões automatizadas, incluindo a definição de perfis, a que se refere o artigo 22.º, n.º 1, ou o tratamento seja suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados na aceção do artigo 35.º.»*

De forma retórica, temos de perguntar: o que se deve entender por *utilização intensiva de dados*? E o que são *motivos razoáveis para presumir que o titular dos dados já*

dispõe das informações? Não podemos concordar com estas exceções à obrigação de fornecer informações que cabe aos responsáveis pelo tratamento, também porque os conceitos indeterminados favorecem a desproteção dos titulares de saber o que as entidades fazem com os seus dados.

5. Em quinto e último lugar, propõe-se alterar o direito do titular dos dados não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, sendo a proposta apresentada no seguinte sentido:

«1. Uma decisão que produza efeitos jurídicos em relação a um titular dos dados ou que o afete significativamente de forma similar só pode basear-se exclusivamente no tratamento automatizado, incluindo a definição de perfis, se essa decisão:

a) For necessária para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento, independentemente de a decisão poder ser tomada por meios não exclusivamente automatizados;

b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e no qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou

c) Se basear no consentimento explícito do titular dos dados.».

Esta alteração proposta reconfigura totalmente a norma, que passa de um direito do titular dos dados para uma permissão de tratamento para o responsável pelo tratamento. Esta total alteração do paradigma normativo leva a que o art. 22.º, integrado no capítulo dedicado aos direitos dos titulares dos dados, fique incorretamente inserido. Uma secção que visa conferir direitos passaria a acolher um artigo que, em bom rigor, é uma base de licitude para o responsável pelo tratamento proceder a novas operações e atividades. Termino, pois, criticando.

Elencadas as 5 principais modificações da proposta que visa alterar o RGPD que considero ser de destacar, tempo é para lançar a décima primeira edição da revista da APDPO.

Boas leituras e vemo-nos na próxima edição!

Inês Oliveira

Presidente da Direção da APDPO

Diretora da DPO Magazine

Notas

Consultar em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52025PC0837, art. 3.º.

Conteúdo

DPO MAGAZINE

n.º 11 | Proteção de Dados, Cibersegurança e Inteligência Artificial

DOSSIER ESPECIAL

Omnibus Digital e desafios do RGPD

- IA responsável: o algoritmo otimiza, o DPO humaniza
- O EPD entre a cibersegurança e a inteligência artificial
- Blockchain, confiança e privacidade desde a conceção
- Fatores humanos e redução de incidentes de dados
- Dados pessoais na indústria musical e nos contratos digitais


AP
DPO
PORTUGAL

DPO MAGAZINE n.º 11

Dossier Especial | Omnibus Digital

Omnibus Digital – o que propõe a Comissão Europeia no que respeita ao RGPD

José Luís Dias

Encontra-se em curso na União Europeia (UE) aquela que poderá ser uma das mais significativas reformas legislativas dos últimos anos no domínio digital. No dia 19 de novembro de 2025 a Comissão Europeia apresentou a sua proposta de "Omnibus Digital", um pacote legislativo que altera um conjunto relevante de legislação digital da UE, incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD), o Regulamento da Inteligência Artificial, a Diretiva ePrivacy ou a Diretiva NIS2. Com o presente artigo procuraremos percorrer as principais propostas de alteração ao RGPD apresentadas, identificando aqueles que são, para a Comissão, os desafios que visam resolver e os benefícios esperados.

O Contexto Político

O Omnibus Digital insere-se numa agenda mais vasta de reforço da competitividade europeia, na sequência dos relatórios Draghi e Letta, que sublinharam a necessidade de eliminar redundâncias normativas, reduzir custos de conformidade e fomentar a inovação. O objetivo declarado pela Comissão é simplificar, harmonizar e clarificar o quadro regulatório digital sem comprometer os elevados padrões de proteção dos direitos fundamentais que distinguem a UE a nível global.

Importa lembrar, no entanto, que esta proposta da Comissão é, apenas, o ponto de partida deste processo legislativo. O Omnibus Digital será agora analisado e negociado pelo Conselho e pelo Parlamento Europeu, que podem introduzir alterações às propostas apresentadas pela Comissão, incluindo eliminar algumas dessas propostas, e até apresentar propostas de alteração a matérias não abordadas pela Comissão.

Dez Matérias em Debate

No que respeita ao RGPD, as alterações propostas incidem sobre dez domínios. Segundo a Comissão, essas propostas visam harmonizar, clarificar e simplificar a aplicação do RGPD, mantendo um elevado nível de proteção de dados em toda a UE, ao mesmo tempo que facilitam o cumprimento do RGPD pelos operadores e apoiam a inovação tecnológica na UE, incluindo o desenvolvimento da inteligência artificial europeia.

1. Conceito de Dados Pessoais e Pseudonimização

Uma das propostas da Comissão mais relevantes, dadas as repercussões que poderá ter, diz respeito à definição de dados pessoais e à sua articulação com o conceito de pseudonimização. Considerando que a definição de dados pessoais constante do RGPD é caraterizada por alguma falta de clareza, nomeadamente quanto ao momento em que se considera que um indivíduo é considerado "indiretamente identificável", a Comissão procura proceder a essa clarificação através da codificação da jurisprudência do Tribunal de Justiça da União Europeia (TJUE). Para tal, a Comissão recupera, sobretudo, a decisão do TJUE no recente caso SRB, onde este tribunal esclareceu que os dados pseudonimizados não devem ser considerados, em todos os casos e para todas as entidades, como dados pessoais para efeitos de aplicação do RGPD, e que a pseudonimização pode, dependendo das circunstâncias do caso, impedir efetivamente que outras pessoas que não o responsável pelo tratamento identifiquem o titular dos dados, de tal forma que, para elas, o titular dos dados não seja ou deixe de ser identificável.

Deste modo, a proposta da Comissão reflete esta jurisprudência: a natureza identificável de um titular deve ser avaliada no momento da recolha e do ponto de vista do responsável pelo tratamento. Adicionalmente, é proposto um mecanismo — através de ato de execução da Comissão, com envolvimento estreito do Comité Europeu para a Proteção de Dados (CEPD) — que especifique os meios e critérios para determinar quando os dados pseudonimizados deixam de constituir dados pessoais para certas entidades. O objetivo com este mecanismo é fornecer às empresas orientações mais claras sobre como gerar dados não pessoais para determinados destinatários, permitindo-lhes ter custos mais baixos quando pretendam recorrer à pseudonimização.

2. Investigação Científica

Com o objetivo de apoiar a investigação e a inovação na Europa, a Comissão apresentou um conjunto de propostas respeitantes à investigação científica, procurando clarificar um conjunto de questões que entende que se suscitam na comunidade científica quanto às condições necessárias para a realização de investigação em conformidade com o RGPD. Deste modo, a proposta de Omnibus Digital prevê:

Uma definição de "investigação científica" para efeitos do RGPD;

Esclarece que a investigação constitui um interesse legítimo para efeitos do princípio da limitação das finalidades;

Esclarece a sua compatibilidade para efeitos de tratamento posterior; e

Prevê salvaguardas adequadas nos casos em que a prestação de informações ao titular seja impossível ou desproporcionada.

3. Tratamento de dados no contexto da Inteligência Artificial

No âmbito da articulação entre proteção de dados e inteligência artificial (IA), a Comissão propõe alterações ao RGPD em duas frentes distintas.

O primeiro conjunto de medidas propostas respeita ao tratamento no contexto do desenvolvimento e do funcionamento da IA, e visa clarificar que o desenvolvimento e o funcionamento de sistemas de IA podem basear-se no interesse legítimo do responsável pelo tratamento (de acordo com o artigo 6.º, n.º 1, alínea f) do RGPD), desde que cumpridas as condições aplicáveis e sujeito a salvaguardas adicionais, nomeadamente medidas técnicas e organizativas e as garantias adequadas para defender os direitos e liberdades do titular dos dados — incluindo a minimização dos dados na fase de seleção das fontes e de treino e testagem de um modelo ou de um sistema de IA, e a proteção contra a divulgação de dados conservados de forma residual.

A segunda proposta apresentada no que respeita à IA prevê, a título excecional, a possibilidade de tratar categorias especiais de dados pessoais quando tal for necessário para o desenvolvimento e funcionamento de um sistema de IA ou de um modelo de IA, desde que seja meramente residual e sujeito a salvaguardas específicas – nomeadamente, a ser aprovada esta proposta, terão de ser aplicadas medidas organizativas e técnicas adequadas para impedir a recolha e outras formas de tratamento de categorias especiais de dados pessoais. Caso, mesmo com essa aplicação, se identificarem dados sensíveis nos conjuntos de dados utilizados para treino, testagem ou validação ou no sistema de IA ou no modelo de IA, esses dados devem ser suprimidos, exceto se essa supressão exigir um esforço desproporcionado, situação em que o responsável pelo tratamento deve proteger eficazmente, sem demora injustificada, esses dados de serem utilizados para produzir resultados, de serem divulgados ou de outro modo disponibilizados a terceiros.

4. Dados Biométricos

No que respeita ao tratamento de dados biométricos, a proposta constante do Omnibus Digital visa uma alteração mais cirúrgica, procurando distinguir de forma mais clara as funções de identificação de um indivíduo (pesquisa de um para muitos) das de confirmação de identidade (isto é, de verificação, ou seja, de comparação de um para um), e introduzindo uma exceção que permite o tratamento de dados biométricos para verificação de identidade, desde que os dados ou os meios necessários à verificação estejam sob o controlo exclusivo do titular.

5. Notificação de Violações de Dados

No âmbito da notificação a efetuar à autoridade de controlo no caso da ocorrência de uma violação de dados pessoais, a Comissão propõe:

Que a notificação ocorra apenas nos casos em que a violação implique um elevado risco para os direitos e liberdades dos titulares – por se entender que as notificações de violação de baixo risco são consideras desnecessariamente onerosas, propõe-se a adoção do critério utilizado para a comunicação aos titulares dos dados;

Alargar o prazo para realização da notificação das 72 horas para as 96 horas;

Que a notificação seja efetuada através de um ponto de entrada único;

Que o CEPD elabore, e a Comissão aprove, quer um modelo comum para a notificação de uma violação de dados pessoais à autoridade de controlo competente quer uma lista das circunstâncias em que uma violação de dados seja suscetível de implicar um elevado risco para os direitos e liberdades de uma pessoa singular.

O objetivo destas alterações é reduzir a carga administrativa dos responsáveis pelo tratamento, aliviar a carga de trabalho das autoridades de supervisão e harmonizar ao nível da UE a noção de "elevado risco" para as violações de dados.

6. Avaliações de Impacto sobre a Proteção de Dados (AIPD)

Atualmente, cada autoridade nacional elabora as suas próprias listas de operações sujeitas ou isentas de AIPD, gerando fragmentação a nível da União dos critérios para realização da avaliação. Com esta proposta, a Comissão procura centralizar em si (através de atos de execução, com base em propostas do CEPD) a aprovação destas listas a nível da União, prevendo ainda a aprovação, nos mesmos termos, de um modelo e de uma metodologia comuns para a realização de AIPD, aumentando a segurança jurídica dos responsáveis pelo tratamento.

7. Obrigações de Informação

Tendo a Comissão considerado que as atuais obrigações de informação dos responsáveis pelo tratamento são desproporcionadas nos casos em que o risco para o titular dos dados é baixo e quando estes já dispõem, na prática, das informações relevantes, veio propor que os responsáveis pelo tratamento fiquem isentos de fornecer determinadas informações quando o tratamento não seja suscetível de resultar em elevado risco e existam motivos razoáveis para supor que o titular já dispõe dessas informações. De acordo com a Comissão, esta é uma medida que beneficia especialmente pequenos operadores com tratamentos de baixo risco, para os quais as obrigações de informação podem causar uma carga desproporcional.

8. Direito de Acesso

A proposta da Comissão visa introduzir a possibilidade de o responsável pelo tratamento recusar dar seguimento a um pedido de acesso ou cobrar uma taxa razoável quando estiver perante pedidos de acesso manifestamente abusivos e para fins que não sejam a proteção dos dados pessoais (por exemplo, pedidos formulados com o único intuito de causar danos ao responsável pelo tratamento ou para fins de chantagem para obtenção de lucros financeiros). Procura-se assim oferecer clareza jurídica, nomeadamente sobre como pode o responsável pelo tratamento atuar nos casos em que o direito de acesso é utilizado de forma abusiva pelo titular dos dados, sem comprometer o exercício legítimo do direito de acesso.

9. Decisões Individuais Automatizadas

No que respeita ao regime aplicável às decisões individuais automatizadas, a reformulação do artigo 22.º proposta pela Comissão é significativa - de acordo com a proposta, esta norma deixará de proclamar um direito do titular (de não ficar sujeito a decisões exclusivamente automatizadas) e passa a abordar esta matéria pela perspetiva do responsável pelo tratamento, elencando as condições em que o responsável pelo tratamento pode recorrer ao tratamento automatizado para decisões com efeitos jurídicos. A Comissão justifica esta proposta por entender que proporciona maior segurança jurídica aos responsáveis pelo tratamento, nomeadamente ao clarificar os requisitos relativos à utilização legítima da tomada de decisões individuais automatizadas.

10. Regime de *Cookies*

Por último, no que às alterações ao RGPD diz respeito, a Comissão propõe uma revisão profunda do regime de *cookies*. Tendo em vista combater a "fadiga de consentimento" e a proliferação dos *banners* de *cookies*, é proposta a transferência para o RGPD das regras relativas a cookies que tratem dados pessoais e que atualmente constam da Diretiva *e-Privacy,* deste modo aplicando as regras do RGPD sempre que forem recolhidos dados pessoais. As alterações propostas incluem ainda a manutenção do princípio de que o acesso a um dispositivo requer consentimento, mas alargando as isenções de consentimento para determinados fins de baixo risco; obrigatoriedade de respeitar a recusa de consentimento durante seis meses; e a possibilidade de definição centralizada de preferências de cookies (por exemplo no navegador de internet ou de outros meios técnicos).

Próximos passos

O Omnibus Digital pode representar uma importante alteração do quadro regulatório digital europeu, com particular impacto no regime de proteção de dados. Analisada a proposta da Comissão Europeia, podemos concluir que, se algumas das suas propostas visam simplificar e harmonizar as regras aplicáveis, resolvendo problemas práticos identificados nos anos de aplicação do RGPD, outras transcendem essa caraterização de mera simplificação técnica, assumindo mesmo relevante dimensão política. A proposta da Comissão não será, por isso, certamente a versão final que será aprovada pelos legisladores europeus. O processo legislativo está agora nas mãos do Conselho e do Parlamento Europeu, e o resultado dos seus trílogos negociais determinará a configuração final das alterações e o RGPD que teremos no futuro.

Pacote Digital Omnibus: uma Perspetiva Prática e Otimista

Diogo Alves

Começo esta exposição parafraseando William Hazlitt, ensaísta inglês do século XVIII: *"Morrer é apenas ficar como estávamos antes de termos nascido"*. **Isto é, se não devemos temer a morte, dada a sua inevitabilidade, muito menos deveremos recear uma alteração legislativa.**

Com isto não se pretende afirmar que a adaptação a esta novidade normativa seja inócua. O medo do desconhecido nasce, muitas vezes, da perceção de que a mudança conduzirá a um caos incontrolável. Contudo, antes desta, já enfrentámos outras alterações legislativas — até mais exigentes — e, uma vez implementadas e compreendidas, o receio deu lugar à normalização. Relativizado o tema pela frase inicial, resta-nos encarar esta mudança com curiosidade crítica, reconhecendo que a evolução jurídica faz parte do próprio processo de maturidade regulatória.

Mais do que discutir a pertinência, utilidade ou necessidade de uma simplificação das regras — frequentemente apontada como tendo efeitos adversos na competitividade, conforme referido no Relatório Draghi — **importa, numa perspetiva de DPO, encarar este novo pacote legislativo como uma oportunidade, com o otimismo necessário para enfrentar os desafios que dele decorrem.** Ainda que não seja possível garantir impactos diretos na tão invocada competitividade, **parece assegurada, pela via da simplificação, uma redução de encargos para os Responsáveis pelo Tratamento, com os DPO na linha da frente, bem como a diminuição do tempo excessivo despendido em tarefas que, muitas vezes, não apresentam um benefício proporcional para os titulares dos dados pessoais.**

As estimativas apontam para poupanças na ordem dos mil milhões de euros anuais após a entrada em vigor destas alterações legislativas, permitindo, em consequência, uma aplicação mais eficaz do Regulamento Geral sobre a Proteção de Dados.

Destacarei, assim, dois artigos deste novo pacote legislativo que serão objeto de alteração e que, no meu entender, terão impacto direto no quotidiano de um DPO, pela sua relevância prática e operacional.

Começo pelo **artigo 33.º do RGPD (*Notificação de uma violação de dados pessoais à autoridade de controlo*)**, um dos preceitos em que as alterações assumem maior impacto. Desde logo, importa salientar a transferência do canal de notificação para o balcão único estabelecido pela Diretiva NIS2, permitindo uma submissão única, bem como o alargamento do prazo para 96 horas quando a violação seja suscetível de implicar um risco elevado para os indivíduos. Acresce a este regime a elaboração, pelo Comité Europeu de Proteção de Dados, de um modelo comum e de orientações indicativas sobre circunstâncias de elevado risco, sujeitas a revisão periódica.

Atualmente, em caso de incidente, o DPO é frequentemente obrigado a notificar diversas autoridades, em formatos e prazos distintos, o que gera pressão acrescida e aumenta a probabilidade de falhas. **Com esta alteração, ao centralizar a notificação, o DPO poderá concentrar-se no que é verdadeiramente essencial: a gestão eficaz do incidente e a proteção dos titulares dos dados pessoais**, assegurando respostas mais céleres e reduzindo encargos administrativos.

Numa perspetiva eminentemente prática, esta mudança exigirá o alinhamento dos vários planos de resposta a incidentes, com a necessária padronização dos fluxos internos de recolha de informação. A este propósito, merece destaque o Regulamento DORA, cuja implementação recente obrigou à revisão de procedimentos e práticas internas. No meu caso concreto, essa adaptação permitiu criar modelos de comunicação de incidentes, cuja experiência acumulada será particularmente útil na transposição dos novos requisitos de notificação para o ponto de entrada único.

O reforço da segurança jurídica resulta evidente, beneficiando também as Autoridades de Controlo, que passarão a receber notificações mais relevantes e estruturadas, evitando a sobrecarga causada por comunicações de menor impacto e permitindo uma atuação mais rápida e eficaz.

Uma das críticas apontadas a esta alteração prende-se com a possibilidade de o Responsável pelo Tratamento alegar a inexistência de risco elevado. Ainda assim, deverá constituir um imperativo ético, reputacional e comercial que as organizações adotem uma postura prudente, salvaguardando os direitos e liberdades dos titulares dos dados pessoais, independentemente da interpretação estrita do risco.

O segundo artigo a destacar é o **artigo 35.º do RGPD (*Avaliação de Impacto sobre a Proteção de Dados*)**, que atualmente levanta dúvidas recorrentes quanto à obrigatoriedade da realização de uma AIPD, levando, por vezes, os DPO a recorrer a pareceres externos ou, em último caso, à autoridade de controlo nacional.

A alteração proposta visa a construção de um sistema harmonizado, no qual o CEPD proporá à Comissão Europeia uma lista comum de tratamentos sujeitos a AIPD, uma lista de tratamentos isentos e uma metodologia uniforme de avaliação. **Com este enquadramento europeu, cada DPO terá maior previsibilidade quanto aos casos em que é exigida uma AIPD e à forma da sua execução,** reduzindo trabalho redundante e riscos de incumprimento.

A segurança jurídica é, assim, reforçada, tornando os processos mais céleres, simples e eficazes. Importa, contudo, sublinhar que, face à rápida evolução tecnológica, estas listas e metodologias deverão ser revistas, pelo menos, de três em três anos, ou sempre que necessário.

Esta alteração tenderá a reduzir a sobrecarga atualmente associada às AIPD, num dos mecanismos centrais do RGPD, com impacto direto na proteção efetiva dos titulares dos dados pessoais.

Da análise destes dois artigos resulta claro que, para além da agenda de competitividade digital europeia, apenas o atual contexto político tem permitido alcançar este nível de consenso regulatório — confirmando que, por vezes, há males que vêm por bem. Ainda que a letargia europeia em

matéria de competitividade seja um obstáculo reconhecido, não deve confundir-se excesso de regulamentação com atraso civilizacional, pois a defesa dos direitos fundamentais continua a ser um pilar essencial de uma sociedade democrática e crítica.

Mesmo admitindo que estas alterações possam comportar algum risco de desregulação, caberá sempre ao DPO assegurar a salvaguarda dos direitos fundamentais dos titulares dos dados pessoais, colocando-se, tanto quanto possível, na sua posição aquando da tomada de decisões.

Em conclusão, numa perspetiva prática, este pacote legislativo promete ganhos significativos em eficiência, redução de burocracia e reforço da segurança jurídica, libertando recursos para atividades que efetivamente acrescentam valor. **Ainda que a simplificação possa, à primeira vista, parecer "*tout court*", não representa um livre-trânsito, exigindo dos DPO, das equipas e dos departamentos envolvidos um planeamento atempado da adaptação dos sistemas internos de proteção de dados pessoais.**

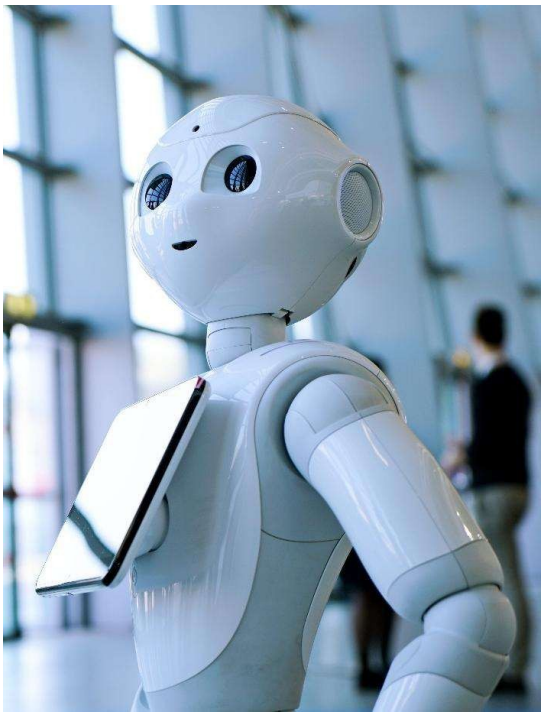
Não obstante o tom otimista desta análise, as eventuais limitações deste pacote legislativo deverão ser progressivamente densificadas pela interpretação dos DPO e das autoridades de controlo nacionais, sempre com o foco primordial no interesse do titular dos dados pessoais.

DPO MAGAZINE n.º 11

Inteligência Artificial e Governação Digital

O algoritmo otimiza, o DPO humaniza!

Sónia Neves | DPO, Zurich Portugal



A Inteligência Artificial (IA) já faz parte do quotidiano das nossas vidas e das organizações, apoiando decisões e processos em áreas como recursos humanos, pricing, deteção de fraude, análise de risco e relacionamento com os clientes.

Sabemos que o potencial é elevado, porém os riscos para os direitos fundamentais das pessoas, titulares dos dados, são igualmente reais.

O maior risco da IA não está na tecnologia em si, mas nas escolhas humanas que orientam a sua criação, implementação e utilização.

Como exemplo, o conhecido *Paperclip Problem* serve de alerta: objetivos aparentemente inofensivos no recurso à IA tendem rapidamente a escalar para consequências desproporcionadas quando faltam limites claros de supervisão humana e mecanismos de governação efetivos.

É neste enquadramento, que o papel de Data Protection Officer (DPO) assume uma relevância estratégica. Para além de assegurar conformidade legal, é necessário que atue também como garante de responsabilidade, transparência e equilíbrio entre inovação e proteção de direitos humanos.

Sabe-se que os sistemas de IA amplificam riscos já conhecidos do Regulamento Geral sobre a Proteção de Dados (RGPD), como a opacidade, o enviesamento, a reutilização indevida de dados e decisões automatizadas, com impacto significativo nos titulares de dados.

Em setores fortemente dependentes de dados pessoais, como os setores segurador, financeiro, saúde ou recursos humanos, estes riscos são particularmente relevantes.

E é por isso que terá de haver uma governação responsável de IA, assente em princípios claros, tais como, a identificação e registo centralizado de todos os casos de IA que surjam nas organizações, a classificação de risco proporcional, avaliações de impacto eficazes, validação rigorosa de fornecedores, supervisão humana e monitorização contínua ao longo de todo o ciclo de vida do sistema que recorra à IA.

Na prática, os riscos surgem frequentemente através de sinais de alerta subtis. Por exemplo, promessas de neutralidade de uso de dados pessoais sem qualquer evidência, ausência de documentação, desconhecimento sobre o tratamento de dados ou sistemas sem uma explicabilidade mínima, são “red flags” que exigem intervenção imediata do DPO.

O futuro da IA aponta para sistemas cada vez mais complexos e integrados, acompanhados por um enquadramento regulatório muito exigente.

Neste seguimento, a governação de IA deixa assim de ser um momento isolado e passa a ser um processo contínuo, onde a proteção de dados, cibersegurança e gestão de risco, caminham lado a lado.

Um dos maiores mitos em torno da IA é a ideia de neutralidade. A IA não é neutra. Reflete escolhas humanas, dados históricos, prioridades de negócio e contextos sociais. Ignorar esta realidade é, por si só, um risco.

Cabe ao DPO, em colaboração com as áreas acima mencionadas, garantir que esta falsa neutralidade não se traduz em discriminação, exclusão ou decisões injustas. Questionar enviesamentos, exigir explicabilidade e garantir supervisão humana não é nem nunca poderá ser um entrave à inovação — é uma condição para que a inovação seja legítima e sustentável.

Muitas vezes, o DPO surge como a última linha de defesa entre a eficiência tecnológica e a proteção dos direitos humanos. Quando a pressão é para avançar rápido, escalar soluções ou não perder a oportunidade, é o DPO que tem de levantar a mão e questionar: Temos base legal? Compreendemos o impacto nos titulares dos dados?

Conseguimos explicar a decisão tomada? Esta não é uma função confortável, mas é uma função essencial.

A verdadeira maturidade digital de uma organização mede-se pela forma como responde a estas perguntas, mesmo quando a resposta não é imediata ou fácil.

Neste contexto, o DPO afirma-se como um facilitador de uma inovação responsável, não deixando de acautelar independência, pensamento crítico, empatia e coragem — características que fazem toda a diferença na implementação de todas as salvaguardas seja em âmbito de RGPD como na implementação segura de sistemas que recorram à IA.

Estamos apenas no início da história da IA...

O que está em jogo, não é apenas tecnologia, mas sim valores!

O futuro da IA será moldado pelas decisões humanas que tomamos agora — pelas perguntas que fizermos, pelos limites que impusermos e pela coragem de colocarmos as pessoas, titulares dos dados pessoais, no centro da decisão.

Algoritmos podem até decidir qual o caminho a optar. Porém, proteger direitos humanos, exige liderança, consciência e responsabilidade.

E é precisamente aqui que a função do DPO ganha relevância e faz a diferença nas organizações: como voz ética, como referência de confiança, como garante de que a inovação não acontece à custa da dignidade humana.

Importa reter que a tecnologia evolui, mas a privacidade, a proteção de dados e os direitos dos titulares dos dados consagrados no RGPD não são negociáveis — nem hoje, nem no futuro.

E... quando tudo empurra para avançar mais depressa, o DPO tem a responsabilidade de travar, questionar e garantir que a decisão certa não é sacrificada pela decisão mais fácil.

DPO MAGAZINE n.º 11

Inteligência Artificial e Cibersegurança

O EPD entre a cibersegurança e a inteligência artificial | A articulação com o Responsável pela Cibersegurança no Decreto-Lei n.º 125/2025 e a função prática do Encarregado de Proteção de Dados no Regulamento IA

Luís Ferreira Mendes

A governação digital deixou definitivamente de caber em silos. Em Portugal, o Decreto-Lei n.º 125/2025 veio densificar o modelo de responsabilidade em cibersegurança, impondo às entidades essenciais e importantes a designação de um responsável de cibersegurança com ligação direta à gestão de topo. Ao mesmo tempo, o Regulamento da Inteligência Artificial da União Europeia acrescenta uma nova camada de obrigações sobre sistemas de IA, em especial nos domínios de risco elevado e de impacto sobre direitos fundamentais. Neste novo quadro, o Encarregado de Proteção de Dados não perde relevância: pelo contrário, passa a ocupar um lugar ainda mais crítico na articulação entre conformidade, risco tecnológico e governação.

1. O fim da abordagem em silos

A maturidade regulatória europeia está a empurrar as organizações para um modelo integrado de governação digital. Já não basta ter "proteção de dados" de um lado, "segurança" de outro e "inovação" noutro departamento sem pontos de contacto estáveis. A realidade operacional dos incidentes, dos sistemas automatizados e da gestão de risco mostra precisamente o contrário: os mesmos processos tocam, ao mesmo tempo, segurança da informação, dados pessoais, continuidade de negócio, risco regulatório e, agora, inteligência artificial.

É neste contexto que a relação entre o Encarregado de Proteção de Dados (EPD) e o Responsável pela Cibersegurança deve ser lida. Não se trata de sobreposição de cargos, nem de absorção de competências. Trata-se de uma articulação funcional necessária para que a organização responda com coerência a obrigações que são juridicamente distintas, mas operacionalmente interdependentes.

2. O que o Decreto-Lei n.º 125/2025 veio alterar

O Decreto-Lei n.º 125/2025, publicado a 4 de dezembro de 2025, aprovou o regime jurídico da cibersegurança e transpôs para o ordenamento jurídico português a Diretiva NIS2. O diploma entrou em vigor 120 dias após a publicação, isto é, a 3 de abril de 2026.

Uma das novidades estruturais do diploma é a obrigatoriedade, para entidades essenciais e importantes, de designar um responsável de cibersegurança. O artigo 31.º determina que esse responsável deve ser titular de órgãos de gestão, direção ou administração, ou responder-lhes orgânica e diretamente. O mesmo artigo enumera funções mínimas, entre as quais: propor medidas de gestão de riscos de cibersegurança, prestar informação aos órgãos de supervisão, apoiar o cumprimento de medidas de supervisão e execução, promover uma cultura de cibersegurança, assegurar a gestão de riscos, garantir o cumprimento das obrigações do relatório anual e coordenar as ações do ponto de contacto permanente, quando essa função não seja assegurada por si. O incumprimento dos deveres do artigo 31.º é qualificado como contraordenação muito grave.

Este desenho legal tem uma consequência organizacional importante: a cibersegurança deixou de poder ser tratada apenas como função técnica de suporte; passa a ter um centro formal de responsabilidade com ligação direta à gestão de topo. E é precisamente por isso que o diálogo com o EPD se torna mais exigente.

3. EPD e Responsável pela Cibersegurança: funções diferentes, fronteiras comunicantes

O Decreto-Lei n.º 125/2025 não cria qualquer relação hierárquica entre o EPD e o responsável de cibersegurança, nem faz do segundo uma autoridade sobre matérias de proteção de dados. Também não substitui o regime do RGPD, nem altera a autonomia funcional do EPD. O que faz é obrigar a organização a reconhecer que muitos processos de segurança são simultaneamente operações de tratamento de dados pessoais.

A distinção funcional continua a ser essencial

O Responsável pela Cibersegurança tem o seu centro de gravidade na resiliência, na proteção das redes e sistemas de informação, na prevenção e resposta a incidentes, na gestão do risco cibernético, na cadeia de abastecimento tecnológica e na relação operacional com a autoridade de cibersegurança. O seu foco é técnico-organizativo e operacional, ainda que com ligação clara à governação.

O EPD, por seu lado, mantém a missão própria que resulta do RGPD: informar e aconselhar sobre obrigações em proteção de dados, monitorizar a conformidade, aconselhar sobre avaliações de impacto, cooperar com a autoridade de controlo e atuar como ponto de contacto em matéria de proteção de dados. O seu foco é a licitude, a proporcionalidade, os direitos dos titulares, a demonstração da responsabilidade e a conformidade contínua do tratamento.

Mas as fronteiras materiais cruzam-se todos os dias: basta pensar em logs, gestão de acessos, monitorização de utilizadores, biometria, deteção de anomalias, investigação forense, gestão de vulnerabilidades, conservação de evidências digitais, partilha de indicadores de compromisso, auditorias de fornecedores ou resposta a incidentes. Em quase todos estes domínios há simultaneamente uma dimensão de segurança e uma dimensão de tratamento de dados pessoais.

4. Onde a articulação é obrigatória na prática

A articulação entre estas duas funções deve ser formalizada, e não deixada ao improviso ou à boa vontade individual.

Desde logo, na gestão de risco, o responsável de cibersegurança pode identificar a necessidade de medidas como retenção reforçada de registos, segmentação de acessos, monitorização intensiva, correlação de eventos, análise comportamental ou due diligence técnica de fornecedores. O EPD deve ser chamado a pronunciar-se sobre os limites de proteção de dados dessas mesmas medidas: minimização, necessidade, proporcionalidade, base de licitude, transparência, prazo de conservação, restrições de acesso, utilização secundária e impactos sobre trabalhadores, clientes ou utilizadores.

Depois, na gestão de incidentes, a separação de fluxos já não é sustentável. Nem todo o incidente de cibersegurança é uma violação de dados pessoais, e nem toda a violação de dados pessoais decorre de um incidente qualificado para efeitos do regime de cibersegurança. Mas em muitos casos haverá sobreposição factual e temporal. Isso exige critérios internos claros para qualificação, segmentação, decisão e notificação, com participação articulada do responsável de cibersegurança, do EPD, do apoio jurídico e da gestão de topo. A própria evolução regulamentar portuguesa aponta para essa lógica de interoperabilidade entre canais e autoridades.

Também na gestão documental, a articulação deve ficar inscrita em políticas, procedimentos e matrizes RACI. Um modelo robusto deve prever, pelo menos, a consulta obrigatória do EPD nas medidas de monitorização com impacto relevante sobre pessoas, a participação do responsável de cibersegurança nas DPIA com componente técnica relevante, um procedimento conjunto para incidentes com potencial impacto simultâneo em segurança e proteção de dados, e o reporte periódico consolidado à administração. Trata-se menos de acumular papel e mais de construir evidência organizacional coerente.

5. O que muda com o Regulamento IA

O Regulamento (UE) 2024/1689, o chamado AI Act, entrou em vigor a 1 de agosto de 2024. A aplicação é faseada: várias regras já começaram a produzir efeitos, mas o regime geral torna-se aplicável a 2 de agosto de 2026, com algumas exceções e calendários específicos.

Do ponto de vista da proteção de dados, importa evitar dois erros frequentes: o primeiro é assumir que o AI Act "substitui" o RGPD. Não substitui; os dois instrumentos coexistem e operam em planos diferentes: o RGPD continua a reger o tratamento de dados pessoais; o AI Act regula a colocação no mercado, a disponibilização, a entrada em serviço e o uso de sistemas de IA, com foco na segurança, nos direitos fundamentais e no modelo europeu de uma IA fiável. O segundo erro é supor que o AI Act cria, por si só, um papel autónomo e universal do EPD dentro da governação da IA. Também não é isso que o regulamento faz; o texto do AI Act não transforma o EPD num órgão obrigatório de governação da IA em sentido geral. O papel do EPD resulta, sobretudo, da articulação entre o AI Act e o RGPD, sempre que a IA envolva tratamento de dados pessoais ou gere riscos relevantes para direitos e liberdades.

6. O papel do EPD no AI Act: não é automático, mas é estrutural

O ponto mais relevante está nas obrigações dos revendedores de sistemas de IA de alto risco.

O artigo 26.º do AI Act prevê que, quando aplicável, os revendedores usem a informação fornecida pelo fornecedor para cumprir a obrigação de realizar uma avaliação de impacto sobre proteção de dados ao abrigo do artigo 35.º do RGPD. Isto significa que o AI Act não cria uma DPIA, mas pressupõe e reforça a sua integração operacional em cenários de IA de alto risco.

Por sua vez, o artigo 27.º estabelece a obrigação de realizar uma avaliação de impacto sobre direitos fundamentais para determinados revendedores de sistemas de IA de alto risco, nomeadamente organismos públicos, entidades privadas que prestem serviços públicos e revendedores de certos sistemas previstos no anexo III. O mesmo artigo determina expressamente que, se alguma das obrigações aí previstas já tiver sido cumprida através de uma DPIA feita ao abrigo do RGPD, a avaliação de impacto sobre direitos fundamentais deve complementar essa DPIA.

É aqui que o EPD ganha centralidade prática. Sempre que exista tratamento de dados pessoais e seja exigível uma DPIA, o EPD deve ser consultado nos termos do RGPD. E quando o projeto envolver simultaneamente IA de alto risco e direitos fundamentais, o EPD deixa de ser apenas um interveniente "de privacidade" e passa a ser um elemento de integração metodológica entre a DPIA, a avaliação de impacto sobre direitos fundamentais, os requisitos de transparência, a limitação de finalidades, a minimização e a gestão documental do sistema.

Por outras palavras: o AI Act não "nomeia" o EPD como diretor da IA, mas, em organizações que tratam dados pessoais através de IA de risco elevado, o EPD torna-se uma peça estrutural do modelo de controlo.

7. O peso interpretativo do ecossistema europeu de proteção de dados

O papel do EPD no contexto da IA também está a ser reforçado no plano institucional e interpretativo europeu.

Em julho de 2024, o EDPB adotou a Declaração 3/2024 sobre o papel das autoridades de Proteção de dados no quadro do Regulamento da Inteligência Artificial, defendendo que as autoridades de proteção de dados já dispõem de experiência e competência relevantes para lidar com o impacto da IA nos direitos fundamentais, em especial no direito à proteção de dados, e que por isso devem desempenhar um papel relevante na arquitetura de supervisão do AI Act. Posteriormente, o EDPB prosseguiu este posicionamento no diálogo com o AI Office.

Isto não altera diretamente o estatuto jurídico do EPD dentro das organizações, mas reforça uma leitura prudente: sempre que a IA toque tratamento de dados pessoais, perfis, inferências, decisão assistida ou automatizada, monitorização, biometria ou serviços públicos, a governação da IA sem envolvimento do EPD será, no mínimo, pobre; em muitos contextos, será um erro de desenho.

8. Um modelo recomendável para as organizações

À luz do Decreto-Lei n.º 125/2025 e do AI Act, a solução mais robusta para entidades públicas e privadas não está em fundir papéis, mas em criar uma arquitetura de articulação formal.

Essa arquitetura deveria assentar em cinco eixos.

a) A separação clara de função: o responsável de cibersegurança foca a resiliência e a segurança; o EPD fica a camada de conformidade em proteção de dados.

b) Os mecanismos obrigatórios de interface: um comité de risco digital, desenho de consulta cruzada, matriz de competências e critérios de segmentação.

c) A integração de avaliações: risco de cibersegurança, DPIA, avaliação de impacto sobre direitos fundamentais,

avaliação de terceiros e avaliação contratual não devem ser produzidas como peças isoladas ou desligadas entre si.

d) A governação de incidentes e sistemas de IA: resposta técnica, qualificação jurídica, comunicação regulatória e evidência documental têm de convergir num único processo controlado.

e) O reporte à administração: a gestão deve receber uma visão única sobre o risco tecnológico, o risco regulatório e o risco de direitos fundamentais, e não relatórios isolados que escondem as dependências entre estes temas.

9. Conclusão

O Decreto-Lei n.º 125/2025 e o Regulamento IA não retiram espaço ao Encarregado de Proteção de Dados. O que fazem é alterar o contexto em que o EPD atua. A sua função já não pode ser lida apenas como uma função de controlo formal de conformidade documental. Num ambiente em que a cibersegurança se institucionaliza ao mais alto nível e em que a IA passa a ser regulada por risco e por impacto sobre direitos fundamentais, o EPD afirma-se como figura de ligação entre legalidade, responsabilidade demonstrada, risco tecnológico e proteção efetiva das pessoas.

A mensagem para as organizações é, por isso, simples: o responsável de cibersegurança e o EPD não são concorrentes, nem redundâncias. São funções diferentes, com missões próprias, que só cumprem plenamente o seu papel quando operam em articulação estruturada. Quem persistir numa lógica de silos corre hoje um risco acrescido: falhar simultaneamente na segurança, na conformidade e na governação.

Nota

Este artigo tem natureza técnico-jurídica e de gestão. A aplicação concreta do Decreto-Lei n.º 125/2025, do RGPD e do Regulamento IA deve ser adaptada ao setor, à tipologia da entidade, ao papel desempenhado no ecossistema digital e à natureza dos sistemas utilizados, devendo, nos casos de maior exposição regulatória, ser validada por uma assessoria jurídica especializada, pelo EPD e pelas funções de segurança e risco.

DPO MAGAZINE n.º 11

Tecnologia, Inovação e Privacidade

Será que a Blockchain ainda tem muito a aprender com o RGPD?

Mário Peixinho

O verdadeiro valor da blockchain não está na transparência absoluta, mas na criação de sistemas de confiança onde a privacidade faz parte da arquitetura.

Vivemos um momento curioso na história digital. Por um lado, tecnologias como a blockchain surgiram com a promessa de sistemas descentralizados, transparentes e resistentes à manipulação. Por outro, a União Europeia respondeu ao crescimento da economia digital com um dos quadros legais mais exigentes do mundo na proteção de dados pessoais: o Regulamento Geral sobre a Proteção de Dados (RGPD).

Durante anos, estas duas realidades foram apresentadas como incompatíveis. A blockchain parecia representar um sistema onde tudo ficava registado para sempre, enquanto o RGPD veio reforçar direitos fundamentais como o controlo dos dados pessoais, a limitação da sua utilização e até o direito ao apagamento.

À primeira vista, parecia um choque inevitável entre tecnologia e direitos fundamentais.

Mas, tal como acontece muitas vezes na história da inovação, o que inicialmente parece um conflito acaba por revelar algo mais interessante: uma oportunidade de evolução.

Hoje começamos a perceber que a questão nunca foi se a blockchain é compatível com o RGPD. A verdadeira questão é outra: como desenhar infraestruturas digitais onde a confiança, a segurança e a privacidade coexistem desde o início.

Durante muito tempo, grande parte do ecossistema blockchain viveu centrado com um conceito simples: visibilidade total. Tudo na cadeia. Tudo transparente. Tudo permanentemente registado.

Este modelo serviu para provar que ativos digitais podiam existir e circular sem intermediários. Foi uma experiência tecnológica importante. Mas o mundo real não funciona assim.

Uma transação económica não é apenas uma transferência entre duas entidades. É um processo que envolve identidades, direitos, obrigações, validações legais e múltiplos intervenientes com diferentes níveis de responsabilidade e acesso à informação. Cada um desses intervenientes precisa de confiar no processo, mas não precisa necessariamente de ver os dados de todos os outros.

A blockchain pode ser vista como um livro de registos. Mas, numa sociedade funcional, nem tudo o que é registado deve ser exposto a todos. Algumas redes funcionam como uma ficha de aptidão médica: garantem e provam que o titular está 'apto' para uma função, sem revelar o histórico clínico ou os exames que levaram a essa conclusão.

É precisamente nesta distinção que a conversa sobre blockchain e RGPD começa a ganhar maturidade.

O RGPD não surgiu para travar a inovação. Surgiu para garantir que a inovação digital respeita direitos fundamentais. O regulamento estabelece princípios claros para o tratamento de dados pessoais: licitude, transparência, minimização de dados, limitação da finalidade e segurança da informação.

Um dos conceitos mais relevantes do RGPD é o de proteção de dados desde a conceção e por defeito. A privacidade não deve ser adicionada no final de um projeto tecnológico. Deve fazer parte da arquitetura desde o primeiro momento.

Este princípio não ficou apenas no RGPD de 2018. A proposta de Regulamento Omnibus, atualmente em discussão na União Europeia, vem reforçar e atualizar este quadro, respondendo às realidades tecnológicas que entretanto emergiram, entre elas, precisamente, as tecnologias de registo distribuído. O Omnibus reconhece que a escala e a natureza da economia de dados mudaram, e que os mecanismos de supervisão, responsabilidade e interoperabilidade precisam de acompanhar essa mudança.

Neste contexto, a blockchain não é o problema. Pode ser parte da solução, desde que concebida com os princípios certos desde o início.

Uma das respostas mais interessantes a esta tensão surgiu através do conceito de Identidade Auto-Soberana, ou Self-Sovereign Identity.

Neste modelo, a blockchain deixa de ser um local onde dados pessoais são armazenados. Em vez disso, passa a funcionar como uma infraestrutura de verificação.

Os dados pessoais permanecem sob controlo do próprio cidadão, normalmente guardados numa carteira digital. A blockchain apenas permite verificar se uma credencial foi realmente emitida por uma entidade legítima.

Podemos pensar numa analogia simples.

Quando mostramos a carta de condução a um agente da autoridade, o objetivo não é entregar toda a nossa informação pessoal. O objetivo é provar algo específico: que estamos autorizados a conduzir.

A lógica das credenciais verificáveis segue exatamente este princípio. Em vez de partilhar todos os dados, partilha-se apenas a prova necessária.

A tecnologia deixa assim de ser um mecanismo de exposição de dados e passa a ser uma infraestrutura de confiança descentralizada.

Esta visão não é apenas teórica. Está a ser aplicada na estratégia digital da União Europeia.

Um dos princípios orientadores é o chamado Once-Only. A ideia é simples: cidadãos e empresas não devem ter de entregar a mesma informação repetidamente a diferentes entidades públicas. Os dados devem poder ser reutilizados entre administrações desde que exista consentimento e controlo do titular.

Para suportar este modelo, a União Europeia está a desenvolver a Carteira de Identidade Digital Europeia, conhecida como EUDI Wallet.

Esta carteira permitirá aos cidadãos armazenar credenciais digitais verificáveis como documentos de identidade, diplomas académicos ou licenças profissionais.

O ponto fundamental é que o cidadão passa a estar no centro do sistema. As instituições deixam de ser os únicos repositórios de informação pessoal e passam a atuar como emissores e verificadores de credenciais.

A blockchain pode aqui funcionar como uma camada de confiança que garante autenticidade e integridade sem expor os dados pessoais.

O verdadeiro valor destas tecnologias não está na promessa de eliminar intermediários ou tornar tudo público. Está na possibilidade de criar infraestruturas digitais onde diferentes entidades conseguem coordenar-se em torno de processos confiáveis.

Em muitos setores, desde o imobiliário à saúde ou à mobilidade, o problema principal não é falta de dados. É falta de confiança entre sistemas diferentes.

Hoje temos bases de dados fragmentadas, informação duplicada, validações manuais e processos burocráticos que consomem tempo e recursos.

A blockchain, quando aplicada com respeito pelos princípios do RGPD, pode funcionar como uma camada de integridade partilhada, permitindo que diferentes entidades confiem no mesmo processo sem terem de expor toda a informação.

No fundo, estamos a assistir à passagem de um modelo onde os dados estavam dispersos e fora do controlo das pessoas para um modelo onde a identidade digital pode voltar a estar nas mãos do próprio cidadão.

E talvez essa seja a verdadeira promessa desta tecnologia: não apenas descentralizar sistemas, mas devolver soberania digital às pessoas.

Esta discussão está longe de terminar. À medida que a inteligência artificial passa a mediar cada vez mais decisões, desde o acesso a serviços até à avaliação de crédito ou à triagem de candidatos, a questão da soberania sobre os dados pessoais torna-se ainda mais premente. Os modelos aqui explorados, credenciais verificáveis, privacidade desde a conceção, controlo pelo cidadão, não são apenas respostas à blockchain. São a fundação sobre a qual a IA responsável também terá de ser construída.

A pergunta que fica: enquanto profissionais de proteção de dados, estamos a participar na conceção dessas fundações ou vamos, mais uma vez, chegar depois da arquitetura já estar feita?

DPO MAGAZINE n.º 11

Fatores Humanos e Cultura de Privacidade

Da Aviação à Privacidade: Como Fatores Humanos Podem Reduzir 70-94% dos Incidentes de Dados

Anderson Andrade

Em 2023, a Europa registou mais de 100.000 notificações de violações de dados às autoridades de proteção de dados, segundo dados da Comissão Europeia. Apesar de cinco anos de RGPD, investimentos crescentes em compliance e formação contínua de colaboradores, as violações de dados não apenas persistem — continuam a aumentar. Por que razão organizações que cumprem todos os requisitos regulamentares, que implementam políticas robustas e que formam regularmente as suas equipas continuam a sofrer incidentes de privacidade?

A resposta mais comum é "erro humano". Um colaborador enviou um email para o destinatário errado. Um técnico de TI configurou mal as permissões de acesso. Um gestor partilhou dados sensíveis numa reunião inadequada. Um funcionário estava sob grande pressão. A solução habitual? Mais formação. Mais políticas. Mais controlos. No entanto, esta abordagem ignora uma lição fundamental que a aviação civil aprendeu há mais de 50 anos: **o erro humano não é a causa raiz — é o sintoma de interfaces mal desenhadas entre humanos e sistemas**.

Quando um avião cai, a investigação não se limita a identificar "erro do piloto". A aviação compreendeu que pilotos altamente treinados, experientes e motivados cometem erros quando as interfaces entre humanos, máquinas, procedimentos e ambiente organizacional não são adequadamente desenhadas. Esta mudança de paradigma — de culpar indivíduos para redesenhar sistemas — transformou a aviação na indústria mais segura do mundo. Hoje, a probabilidade de morrer num acidente de avião comercial é de 1 em 11 milhões, segundo a International Air Transport Association (IATA).

E se aplicássemos os mesmos princípios de fatores humanos à proteção de dados? E se, em vez de culpar o colaborador que enviou o email errado, investigássemos **por que razão** a interface entre esse colaborador e o sistema de email tornou esse erro tão fácil de cometer? E se, em vez de mais formação genérica, redesenhássemos as interfaces críticas onde as violações de dados realmente ocorrem?

Foi precisamente esta questão que me levou a desenvolver dois frameworks complementares — **SHELL-Privacy™** e **MEDA-Privacy™** — que adaptam metodologias comprovadas da aviação civil para o contexto da proteção de dados. Ao longo de cinco anos, aplicando estes frameworks em mais de 20 organizações de setores diversos (saúde, tecnologia, serviços financeiros, administração pública), observei reduções consistentes de 70-94% em incidentes recorrentes de privacidade e aumentos significativos no reporte voluntário de quase-incidentes — um indicador-chave de cultura de segurança saudável.

SHELL-Privacy™: Mapeando Onde as Violações Realmente Ocorrem

O modelo SHELL foi desenvolvido na década de 1970 por Elwyn Edwards e posteriormente refinado por Frank Hawkins para a aviação. O acrónimo representa cinco componentes de um sistema: **Software** (procedimentos, regulamentos), **Hardware** (equipamentos, tecnologia), **Environment** (ambiente organizacional), **Liveware** (ser humano central) e **Liveware** (outros seres humanos). O modelo SHELL não analisa componentes isoladamente — analisa as **interfaces** entre eles, reconhecendo que a maioria dos acidentes ocorre quando estas **interfaces** são mal desenhadas.

Adaptei este modelo para criar o **SHELL-Privacy™**, que mapeia sistematicamente cinco interfaces críticas onde violações de dados ocorrem:

Interface Liveware-Software (L-S): Como Humanos Interagem com Sistemas e Aplicações

Esta interface examina como colaboradores interagem com sistemas de TI, aplicações, bases de dados e plataformas digitais. Violações de dados frequentemente ocorrem não porque os sistemas são inseguros, mas porque a interface entre humanos e sistemas torna o erro fácil e o comportamento correto difícil.

Considere-se um caso real que investiguei: uma organização de saúde sofreu uma violação quando uma enfermeira partilhou acidentalmente o ficheiro errado com um paciente. A investigação tradicional concluiria "erro humano" e recomendaria "mais formação em proteção de dados". A análise **SHELL-Privacy™** revelou que o sistema de gestão de documentos apresentava ficheiros de pacientes diferentes em janelas visualmente idênticas, sem indicadores visuais claros de qual ficheiro estava ativo. Sob pressão de tempo (a enfermeira tinha 12 pacientes aguardando atendimento), com interrupções constantes (telefone a tocar, colegas a solicitar ajuda) e num ecrã de computador mal posicionado (luz solar criava reflexos), o erro era não apenas previsível — era inevitável.

A solução não foi mais formação. Redesenhámos a interface: cores distintas para ficheiros de pacientes diferentes, confirmação obrigatória antes de partilhar (mostrando nome completo do paciente e tipo de documento), e indicadores visuais proeminentes do ficheiro ativo. Nos 18 meses seguintes, este tipo de incidente não voltou a ocorrer.

Interface Liveware-Liveware (L-L): Como Equipas Comunicam e Colaboram

Esta interface analisa como informação flui entre pessoas — comunicação verbal, escrita, formal, informal. Violações de dados frequentemente resultam de falhas de comunicação entre equipas, departamentos ou níveis hierárquicos.

Num caso que investiguei numa instituição financeira, dados pessoais de clientes foram inadvertidamente incluídos num relatório partilhado com auditores externos. A investigação tradicional identificou "erro do analista" que preparou o relatório. A análise **SHELL-Privacy™** revelou uma falha na interface L-L: o pedido do gestor ao analista foi verbal, ambíguo ("prepara um relatório com os dados da campanha") e feito sob pressão de prazo. O analista, recém-contratado, não tinha clareza sobre o que "dados da

campanha" significava e sentiu-se desconfortável em questionar o gestor (dinâmica de poder). Não existia checklist ou template para este tipo de relatório, nem revisão por pares antes de partilha externa.

A solução envolveu redesenhar a interface L-L: templates padronizados para relatórios externos, checklist de verificação de dados pessoais, revisão obrigatória por segundo analista, e normalização da prática de "questionar para clarificar" como comportamento esperado e valorizado (não como sinal de incompetência).

Interface Liveware-Hardware (L-H): Como Humanos Interagem com Dispositivos Físicos

Esta interface examina como colaboradores interagem com dispositivos físicos — computadores, smartphones, impressoras, dispositivos de armazenamento, controlos de acesso físico. Violações frequentemente ocorrem quando o design de hardware não considera limitações e comportamentos humanos naturais.

Investiguei um caso numa universidade onde documentos confidenciais de alunos foram deixados numa impressora partilhada e recolhidos por pessoa não autorizada. A investigação tradicional culpou o docente por "negligência". A análise **SHELL-Privacy™** revelou que a impressora estava localizada a 50 metros do gabinete do docente, num corredor movimentado, e o tempo médio entre enviar impressão e recolher documentos era de 3-5 minutos (durante os quais o docente frequentemente era interrompido por alunos ou colegas). O sistema de impressão não oferecia opção de "impressão segura" (libertação mediante código PIN na impressora).

A solução não foi disciplinar o docente. Implementámos impressão segura obrigatória para documentos classificados como confidenciais (deteção automática baseada em metadados), relocalizámos impressoras para áreas de acesso controlado, e criámos alertas visuais no ecrã quando documentos aguardavam recolha há mais de 2 minutos.

Interface Liveware-Environment (L-E): Como Ambiente Organizacional Influencia Decisões

Esta interface analisa como pressões organizacionais, cultura, recursos, carga de trabalho e ambiente físico influenciam decisões relacionadas com privacidade.

Violações frequentemente ocorrem quando colaboradores enfrentam pressões que tornam atalhos atrativos ou quando recursos inadequados tornam o comportamento correto impraticável.

Investiguei um caso numa empresa de tecnologia onde um engenheiro partilhou dados de produção (contendo dados pessoais) com ambiente de desenvolvimento para acelerar testes. A investigação tradicional concluiu "violação intencional de política" e resultou em ação disciplinar. A análise **SHELL-Privacy™** revelou que a interface L-E estava severamente desalinhada: a empresa tinha prazo contratual apertado com cliente (pressão de tempo), o processo aprovado para anonimização de dados demorava 2 semanas (recurso inadequado), e a cultura organizacional valorizava explicitamente "entregar rápido" sobre "seguir processos" (mensagem contraditória da liderança).

A solução envolveu redesenhar a interface L-E: automatização do processo de anonimização (redução de 2 semanas para 2 horas), alocação de recursos dedicados para suporte a privacidade, e mudança de mensagem da liderança para "**entregar rápido e com privacidade**" (não "ou"). Crucialmente, o engenheiro não foi punido — foi reconhecido por ter identificado um gargalo crítico no processo.

Interface Software-Software (S-S): Como Sistemas Integram e Partilham Dados

Esta interface examina como sistemas de TI comunicam entre si, partilham dados, sincronizam informação e aplicam controlos de acesso. Violações frequentemente ocorrem em integrações entre sistemas, APIs, migrações de dados e sincronizações automáticas.

Investiguei um caso numa organização de saúde onde dados de pacientes foram inadvertidamente expostos através de API. A investigação tradicional identificou "erro de configuração" pela equipa de TI. A análise **SHELL-Privacy™** revelou que a interface S-S tinha falhas de design: a API herdava permissões de acesso do sistema de origem (que tinha controlos menos restritivos), não existia documentação clara sobre que dados a API expunha, e o processo de revisão de segurança de APIs não incluía análise de privacidade (apenas segurança técnica).

A solução envolveu redesenhar a interface S-S: princípio de "permissões explícitas" para todas as APIs (nunca herdar), documentação obrigatória de fluxos de dados pessoais, e integração de privacy review no processo de aprovação de APIs. Implementámos também monitorização automatizada de APIs para detetar exposições não intencionais de dados pessoais.

MEDA-Privacy™: Investigando Incidentes sem Culpa

Identificar onde violações ocorrem (**SHELL-Privacy™**) é apenas metade da solução. Quando incidentes acontecem, precisamos de investigá-los de forma que gere aprendizagem organizacional genuína, não apenas identificação de "culpados". Foi aqui que adaptei o **MEDA** (Maintenance Error Decision Aid), uma metodologia de investigação desenvolvida pela Boeing para a aviação.

O **MEDA** foi criado reconhecendo que investigações tradicionais de acidentes na aviação frequentemente paravam em "erro do mecânico" sem compreender **por que razão** mecânicos altamente treinados e experientes cometiam erros. O **MEDA** estrutura investigações em cinco fases que progressivamente aprofundam a análise, movendo de "o que aconteceu" para "por que aconteceu" e finalmente "como prevenir recorrência".

O **MEDA-Privacy™** adapta esta metodologia para violações de dados:

Fase 1: Investigação do Evento

Esta fase estabelece os factos: o que aconteceu, quando, onde, quem estava envolvido, que dados foram afetados, que sistemas estavam envolvidos. Crucialmente, esta fase é descritiva, não avaliativa. O objetivo é compreender a sequência de eventos sem julgamento.

Num caso que investiguei, a Fase 1 estabeleceu: "No dia 15 de março, às 14:35, a analista Maria enviou email contendo dados pessoais de 47 clientes para endereço externo incorreto. O email continha nome, morada, Cadastro de Pessoa Física (CPF/NIF) e histórico de compras. O erro foi detetado 2 horas depois quando o destinatário correto questionou a ausência do email esperado."

Fase 2: Análise de Erro

Esta fase identifica que tipo de erro ocorreu, utilizando taxonomia de fatores humanos. Erros podem ser de execução (ação correta executada incorretamente),

planeamento (ação errada planeada) ou violação (desvio intencional de procedimento). Cada tipo de erro tem causas e soluções diferentes.

No caso da analista Maria, a Fase 2 identificou "erro de execução": Maria planeou corretamente enviar email para cliente A, mas executou incorretamente ao selecionar cliente B (nomes similares na lista de contactos). Não foi erro de planeamento (ela sabia para quem enviar), nem violação (ela não ignorou intencionalmente procedimento).

Fase 3: Análise de Decisão

Esta fase investiga **por que razão** a pessoa tomou as decisões que tomou no momento. Que informação estava disponível? Que pressões existiam? Que alternativas foram consideradas? Esta fase assume que, no momento, a decisão fez sentido para a pessoa — o nosso trabalho é compreender o contexto que tornou essa decisão lógica.

No caso da Maria, a Fase 3 revelou: Maria estava a processar 15 pedidos de clientes simultaneamente (carga de trabalho elevada), tinha sido interrompida 3 vezes por telefone enquanto preparava o email (interrupções), os nomes dos clientes A e B eram "João Silva" e "João Silveira" (similaridade), e o sistema de email não oferecia confirmação visual clara de destinatário selecionado (interface inadequada). No contexto de Maria naquele momento — carga elevada, interrupções, nomes similares, interface ambígua — o erro era altamente provável.

Fase 4: Análise de Fatores Sistémicos

Esta fase investiga as condições organizacionais que criaram o contexto para o erro: políticas, procedimentos, recursos, formação, cultura, pressões de negócio e design de sistemas. Esta é a fase mais crítica, pois identifica as causas raiz sistémicas.

No caso da Maria, a Fase 4 identificou múltiplos fatores sistémicos: a equipa estava subdimensionada (3 analistas para volume de trabalho que requeria 5), não existia sistema de gestão de filas de pedidos (analistas geriam pedidos manualmente em Excel), o sistema de email não tinha funcionalidade de confirmação de destinatário para emails com dados sensíveis, e a cultura organizacional valorizava "responder rápido" sobre "verificar cuidadosamente" (pressão de tempo).

Fase 5: Ações Corretivas

Esta fase desenha intervenções que redesenham interfaces identificadas como problemáticas. Ações corretivas eficazes são sistémicas (mudam o sistema, não apenas treinam pessoas), específicas (endereçam causas raiz identificadas) e mensuráveis (permitem verificar eficácia).

No caso da Maria, as ações corretivas incluíram: contratação de 2 analistas adicionais (reduzir carga de trabalho), implementação de sistema de gestão de filas (eliminar gestão manual em Excel), configuração de confirmação obrigatória de destinatário para emails contendo dados classificados como sensíveis (redesenhar interface L-S), e mudança de métricas de desempenho de "tempo de resposta" para "precisão e tempo de resposta" (mudar cultura).

Crucialmente, Maria não foi disciplinada. Foi reconhecida por ter reportado o incidente prontamente (permitindo mitigação rápida) e por ter participado construtivamente na investigação. Nos 12 meses seguintes, este tipo de incidente reduziu 89% na organização.

Resultados: Da Teoria à Prática

Ao longo de cinco anos aplicando **SHELL-Privacy™** e **MEDA-Privacy™** em mais de 20 organizações, observei padrões consistentes de resultados. Organizações que implementaram ambos os frameworks reportaram reduções de 70-94% em incidentes recorrentes de privacidade. Igualmente importante, reportaram aumentos significativos no reporte voluntário de quase-incidentes — situações onde uma violação quase ocorreu mas foi evitada.

Este segundo indicador é particularmente revelador. Na aviação, altas taxas de reporte de quase-incidentes são consideradas sinal de cultura de segurança saudável: colaboradores sentem-se seguros em reportar problemas porque sabem que o foco será em aprender e melhorar sistemas, não em culpar indivíduos. Quando organizações mudam de investigações punitivas para investigações de aprendizagem (**MEDA-Privacy™**), colaboradores começam a reportar proativamente situações de risco, permitindo intervenções preventivas antes que violações ocorram.

Um padrão particularmente interessante emergiu: organizações que implementaram apenas **SHELL-Privacy™** (mapeamento de interfaces) sem **MEDA-Privacy™** (investigação blameless) obtiveram melhorias modestas (20-30% redução em incidentes). Organizações que implementaram apenas **MEDA-Privacy™** sem **SHELL-Privacy™** obtiveram melhorias similares. No entanto, organizações que implementaram ambos os frameworks de forma integrada obtiveram melhorias dramaticamente superiores (70-94% redução). Esta sinergia sugere que mapear onde violações ocorrem e investigar por que ocorrem são competências complementares que se reforçam mutuamente.

Implicações para DPOs: Além do Compliance

Para Data Protection Officers, estes frameworks oferecem ferramentas práticas que complementam abordagens tradicionais de compliance. O RGPD exige que organizações implementem "medidas técnicas e organizativas adequadas" para garantir segurança de dados pessoais. **SHELL-Privacy™** fornece metodologia estruturada para identificar sistematicamente onde essas medidas são necessárias, analisando interfaces críticas em vez de confiar em checklists genéricos.

O RGPD também exige que organizações mantenham registos de violações de dados e implementem medidas para prevenir recorrência. **MEDA-Privacy™** fornece metodologia estruturada para investigações que não apenas cumprem requisitos regulamentares, mas geram aprendizagem organizacional genuína que previne recorrências.

Crucialmente, estes frameworks mudam a conversa com a liderança organizacional. Em vez de apresentar violações de dados como "erro humano" (implicando que colaboradores são o problema), DPOs podem apresentar violações como "falhas de interface" (implicando que sistemas precisam de redesign). Esta mudança de narrativa é poderosa: líderes organizacionais compreendem investimento em redesign de sistemas; resistem a narrativas que culpam colaboradores.

Implementar estes frameworks não requer orçamentos significativos ou tecnologias complexas. Requer mudança de mentalidade: de "culpar e treinar" para "compreender e redesenhar". Requer que DPOs desenvolvam competências básicas de fatores humanos: observar como colaboradores realmente trabalham (não como políticas assumem que trabalham), questionar por que erros fazem sentido no contexto onde ocorrem, e desenhar intervenções que tornam o comportamento correto o caminho de menor resistência.

Conclusão: Repensando "Erro Humano"

Cinquenta anos de aviação civil ensinaram uma lição fundamental: humanos são falíveis, mas sistemas podem ser desenhados para acomodar essa falibilidade. Pilotos cometem erros, mas aviões modernos têm múltiplas camadas de proteção que tornam esses erros não-catastróficos. Mecânicos cometem erros, mas procedimentos de manutenção são desenhados assumindo que erros ocorrerão e criando verificações que os detetam antes que causem acidentes.

A proteção de dados pode aprender a mesma lição. Colaboradores cometerão erros — enviarão emails para destinatários errados, configurarão mal permissões, partilharão dados inadequadamente. A questão não é se erros ocorrerão (ocorrerão), mas se os nossos sistemas são desenhados para prevenir, detetar e mitigar esses erros antes que se tornem violações de dados.

SHELL-Privacy™ e **MEDA-Privacy™** oferecem caminhos práticos para essa mudança de paradigma. Não substituem compliance, formação ou políticas — complementam-nos com foco sistemático em fatores humanos. Não eliminam erro humano (impossível) — redesenham interfaces para tornar erros menos prováveis e menos consequentes.

Para DPOs e profissionais de privacidade que desejam aprofundar estes frameworks, escrevi quatro livros (disponíveis em português, inglês, francês e espanhol — disponíveis na Amazon.com) que detalham metodologias, ferramentas práticas, estudos de caso e guias de implementação. No entanto, o mais importante não são os livros ou os frameworks — é a mudança de mentalidade que representam.

Quando a próxima violação de dados ocorrer na vossa organização, resistam à tentação de parar em "erro humano". Perguntem: que interface estava mal desenhada? Que pressões sistémicas tornaram o erro provável? Que podemos redesenhar para prevenir recorrência? As respostas a estas questões transformarão violações de dados de crises recorrentes em oportunidades de aprendizagem que fortalecem sistematicamente os vossos programas de privacidade.

A aviação transformou erro humano em segurança sistemática. A proteção de dados pode fazer o mesmo.

Anderson Andrade

DPO | CISO | Advogado | Autor

Anderson Andrade é Data Protection Officer e Chief Information Security Officer com mais de 5 anos de experiência especializada em privacidade e proteção de dados, complementados por 14 anos como advogado. Certificado como EXIN Data Protection Officer (DPO) e EXIN Privacy & Data Protection Professional (PDPP), desenvolveu os frameworks **SHELL-Privacy™** e **MEDA-Privacy™** adaptando princípios de fatores humanos da aviação civil para proteção de dados.

Aplicou estes frameworks em mais de 20 organizações de setores diversos, obtendo reduções consistentes de 70-94% em incidentes recorrentes de privacidade. Autor de quatro livros sobre privacidade e fatores humanos publicados em português, inglês, francês e espanhol. Atua como consultor independente em privacidade, cibersegurança e fatores humanos na Privacy Default Consulting LLM.

Contacto:
https://www.linkedin.com/in/andersonandradeshellprivacy/

Telemóvel: +1 (647) 671-5067

Disponível na Amazon.com: https://amzn.to/44mnkiv

DPO MAGAZINE n.º 11

Estudos Jurídicos

A Tutela Jurídica dos Dados Pessoais Face à Progressiva Digitalização: Evolução Legislativa e Desafios Jurídicos

Anaís de Menezes Leitão

A progressiva digitalização tem colocado novos desafios à tutela jurídica dos dados pessoais, impondo uma constante atualização legislativa e uma leitura integrada entre proteção de dados, direito do consumo e contratação digital. A tutela jurídica dos dados pessoais deixou de poder ser vista apenas como uma dimensão da privacidade: assume hoje a natureza de verdadeiro direito fundamental, com relevância autónoma e transversal nas relações jurídicas contemporâneas.

Esse reconhecimento encontra consagração expressa no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, segundo o qual todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. A Carta acrescenta que esses dados devem ser objeto de tratamento leal, para fins determinados e com fundamento legítimo, ficando o cumprimento destas regras sujeito ao controlo de uma autoridade independente.

A autonomização da proteção de dados relativamente ao direito à vida privada revela a importância crescente da informação pessoal na sociedade digital. Na prática, os dados pessoais passaram a ocupar um lugar central na organização da economia, na prestação de serviços, na relação entre consumidores e plataformas e na própria construção da identidade digital dos cidadãos.

1. A evolução do quadro jurídico europeu

Foi neste contexto que surgiu o Regulamento (UE) 2016/679, de 27 de abril de 2016, comummente designado Regulamento Geral sobre a Proteção de Dados (RGPD), aplicável desde 25 de maio de 2018. O RGPD veio substituir a Diretiva 95/46/CE e reforçar a harmonização europeia em matéria de proteção das pessoas singulares relativamente ao tratamento de dados pessoais e à livre circulação desses dados.

A opção por um regulamento, diretamente aplicável nos Estados-Membros, procurou ultrapassar as assimetrias resultantes da transposição nacional da Diretiva 95/46/CE. Embora o RGPD admita margens de concretização nacional, o seu objetivo foi estabelecer um regime comum, assente em princípios como a licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade pelo cumprimento.

Em Portugal, a Lei n.º 58/2019, de 8 de agosto, assegurou a execução do RGPD no ordenamento jurídico interno. O regulamento consagrou ainda um catálogo reforçado de direitos dos titulares dos dados, incluindo o direito de informação, acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição e proteção perante decisões individuais automatizadas, nos termos aplicáveis.

Para efeitos do RGPD, dados pessoais são qualquer informação relativa a uma pessoa singular identificada ou identificável. Esta definição, constante do artigo 4.º, n.º 1, abrange informação que permita identificar alguém direta ou indiretamente, designadamente por referência a nome, número de identificação, dados de localização, identificadores eletrónicos ou elementos próprios da identidade física, fisiológica, genética, mental, económica, cultural ou social.

2. Dados pessoais e contratos digitais

A evolução tecnológica tornou frequentes contratos digitais celebrados de forma simples, imediata e, muitas vezes, quase impercetível para o consumidor. A criação de uma conta numa rede social, a utilização de uma aplicação, a adesão a uma plataforma de streaming ou o acesso a um serviço digital podem envolver uma relação contratual na qual não existe pagamento em dinheiro, mas existe recolha e tratamento de dados pessoais.

Daqui resulta uma questão central: podem os dados pessoais funcionar, na prática económica, como contrapartida pelo acesso a conteúdos ou serviços digitais? A resposta exige cautela. Os dados pessoais não são uma mercadoria comum, nem podem ser desligados da sua natureza de direito fundamental. Ainda assim, é inegável que têm valor económico e que muitos modelos de negócio digitais assentam na recolha, análise e exploração de informação pessoal.

O problema não está apenas no facto de os dados terem valor económico. Está, sobretudo, na circunstância de muitos titulares não terem plena consciência de que a utilização de determinado serviço implica uma troca: acesso a uma funcionalidade digital em contrapartida da disponibilização, direta ou indireta, de dados pessoais. Essa troca pode ocorrer através de formulários, perfis de utilizador, histórico de navegação, identificadores eletrónicos, cookies ou outros mecanismos de recolha.

Neste ponto, a articulação entre direito da proteção de dados e direito do consumo torna-se particularmente relevante. Do ponto de vista do RGPD, qualquer tratamento de dados pessoais exige fundamento de licitude, informação transparente, respeito pelos princípios aplicáveis e possibilidade de exercício dos direitos do titular. Do ponto de vista do direito do consumo, importa perceber se o consumidor beneficia de meios de reação quando o serviço digital não é fornecido, é defeituoso ou não corresponde ao acordado.

3. Consentimento, transparência e valor económico dos dados

O consentimento, quando utilizado como fundamento de licitude, deve corresponder a uma manifestação de vontade livre, específica, informada e inequívoca. Em determinados casos, o RGPD exige consentimento explícito. Em todos os casos, o titular deve compreender para que finalidades os seus dados são tratados, por quem, durante quanto tempo e com que consequências.

O considerando 42 do RGPD recorda que o consentimento não deve considerar-se livremente prestado se o titular não dispuser de uma escolha verdadeira ou livre, ou se não

puder recusar ou retirar o consentimento sem ser prejudicado. Esta exigência é especialmente importante nos contratos digitais em que a prestação do serviço é apresentada como gratuita, mas depende de tratamentos de dados pessoais que excedem o estritamente necessário à execução do contrato.

O artigo 7.º, n.º 4, do RGPD reforça esta preocupação ao determinar que, na avaliação da liberdade do consentimento, deve ser tida em conta a eventual subordinação da execução de um contrato ao consentimento para tratamentos de dados pessoais que não sejam necessários para essa execução. Trata-se de um ponto essencial para evitar que o consentimento seja transformado numa formalidade sem verdadeira liberdade decisória.

A discussão sobre os dados pessoais como contrapartida deve, por isso, ser enquadrada com rigor. Não se trata de afirmar que os dados pessoais são simplesmente um preço equivalente ao dinheiro. Trata-se de reconhecer que, em certos modelos digitais, a prestação de dados pessoais constitui um elemento económico relevante da relação contratual, devendo o consumidor ser protegido contra práticas opacas, desequilibradas ou desconformes.

4. Do regime clássico dos contratos digitais às Diretivas de 2019

A Diretiva 2011/83/UE, relativa aos direitos dos consumidores, foi durante anos um instrumento relevante no enquadramento dos contratos celebrados à distância e fora do estabelecimento comercial. Porém, a intensificação da contratação digital revelou lacunas quanto ao fornecimento de conteúdos e serviços digitais, sobretudo quando o consumidor não pagava um preço em dinheiro, mas facultava dados pessoais.

Em 2015, a Comissão Europeia avançou com uma proposta destinada a regular certos aspetos dos contratos de fornecimento de conteúdos digitais, procurando reduzir incertezas jurídicas e reforçar a confiança dos consumidores no mercado digital. O objetivo era criar um nível harmonizado de proteção em toda a União Europeia, evitando soluções fragmentadas entre Estados-Membros.

A versão inicial da proposta gerou críticas, designadamente por fazer depender a proteção do consumidor da disponibilização ativa dos dados pessoais. Esta distinção criava dificuldades relevantes: se os dados fossem recolhidos de forma passiva, por exemplo através de determinados mecanismos automáticos, o consumidor poderia ficar fora do âmbito de proteção, apesar de os dados desempenharem a mesma função económica no modelo de negócio.

Essa distinção foi justamente contestada. O critério do fornecimento "ativo" era incerto, difícil de aplicar e potencialmente gerador de incentivos perversos. Na prática, poderia favorecer modelos de recolha menos transparentes, afastando a proteção precisamente quando o consumidor tivesse menor consciência do tratamento dos seus dados.

A Diretiva (UE) 2019/770, publicada em 22 de maio de 2019, suprimiu essa referência ao fornecimento ativo. A versão final passou a abranger os casos em que o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, exceto quando esses dados sejam tratados exclusivamente para fornecer os conteúdos ou serviços digitais ou para cumprir requisitos legais a que o profissional esteja sujeito, sem tratamento para outros fins.

Em Portugal, as Diretivas (UE) 2019/770 e 2019/771 foram transpostas pelo Decreto-Lei n.º 84/2021, de 18 de outubro, que regula os direitos do consumidor na compra e venda de bens, conteúdos e serviços digitais. Este diploma reforçou a proteção do consumidor também nas situações em que o acesso a conteúdos ou serviços digitais é obtido mediante a disponibilização de dados pessoais.

5. Âmbito de aplicação da Diretiva (UE) 2019/770

Nos termos do artigo 3.º da Diretiva (UE) 2019/770, o regime aplica-se aos contratos em que o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e este pague ou se comprometa a pagar o respetivo preço. Aplica-se igualmente quando o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, salvo se esses dados forem tratados exclusivamente para fornecer o conteúdo ou serviço digital ou para cumprir obrigações legais.

São exemplos de conteúdos digitais os ficheiros de música, vídeos, livros eletrónicos ou programas informáticos. Já os serviços digitais abrangem realidades como plataformas que permitem criar, tratar, aceder ou armazenar dados em formato digital, incluindo serviços de cloud, redes sociais, plataformas de partilha de conteúdos, correio eletrónico ou serviços de streaming, consoante o caso concreto.

Quando o conteúdo digital é fornecido através de suporte material utilizado exclusivamente como meio de disponibilização, como uma pen USB ou um DVD, a Diretiva também pode ser aplicável ao conteúdo digital e, em certos termos, ao suporte material. Além disso, os Estados-Membros podem alargar o âmbito de proteção, mas não restringir o núcleo harmonizado imposto pelo direito da União.

6. Falta de conformidade e meios de reação do consumidor

Uma das principais inovações da Diretiva (UE) 2019/770 respeita aos meios de reação em caso de falta de conformidade. Em termos gerais, perante uma desconformidade, o consumidor pode exigir a reposição da conformidade dos conteúdos ou serviços digitais, beneficiar de uma redução proporcional do preço ou resolver o contrato, nas condições legalmente previstas.

A avaliação da conformidade exige comparar a prestação devida, expressa ou implicitamente acordada, com a prestação efetivamente realizada. O profissional responde pelo não fornecimento dos conteúdos ou serviços digitais e pelas faltas de conformidade que existam ou se manifestem nos prazos aplicáveis, tendo especial relevância o tipo de fornecimento contratado: ato único, série de atos individuais ou fornecimento contínuo durante determinado período.

A diferença entre contratos com pagamento de preço e contratos em que o consumidor faculta dados pessoais tem consequências práticas. Nos contratos pagos em dinheiro, a redução do preço é um meio de reação natural. Já nos contratos em que a contrapartida consiste na disponibilização de dados pessoais, a redução do preço pode não ser adequada, assumindo particular importância a reposição da conformidade ou a resolução do contrato, sem prejuízo da aplicação autónoma do RGPD.

Esta articulação é decisiva. O direito do consumo oferece respostas contratuais perante o não fornecimento ou a falta de conformidade. O RGPD, por sua vez, regula a licitude, transparência e proporcionalidade do tratamento de dados pessoais, bem como os direitos do titular, incluindo o direito de retirar o consentimento quando este seja o fundamento de licitude utilizado.

7. A articulação necessária com o RGPD

A Diretiva (UE) 2019/770 não substitui nem reduz as exigências do RGPD. Pelo contrário, o seu artigo 3.º, n.º 8, estabelece que o direito da União em matéria de proteção de dados pessoais se aplica a todos os dados pessoais tratados no âmbito dos contratos abrangidos e que, em caso de conflito, prevalece esse regime de proteção de dados.

Daqui resulta uma consequência importante: o facto de os dados pessoais poderem ser relevantes na economia do contrato digital não permite ignorar os princípios do RGPD. O profissional que fornece o conteúdo ou serviço digital pode, simultaneamente, assumir a qualidade de responsável pelo tratamento. Nessa qualidade, deve assegurar base de licitude, transparência, minimização, segurança, limitação da conservação e demonstração da conformidade.

Também não basta informar genericamente que os dados serão tratados. A informação deve ser clara, acessível e adequada ao titular. Sempre que existam tratamentos para finalidades distintas da execução do contrato - por exemplo, publicidade comportamental, definição de perfis, partilha com terceiros ou monetização indireta -, esses tratamentos devem ser analisados autonomamente à luz do RGPD.

A proteção do consumidor e a proteção dos dados pessoais não devem, por isso, ser vistas como regimes concorrentes. São regimes complementares. O primeiro responde ao desequilíbrio típico da relação consumidor-profissional e à necessidade de conformidade do serviço. O segundo protege o titular enquanto pessoa singular, garantindo controlo, transparência e limites ao tratamento da sua informação pessoal.

Conclusão

A progressiva digitalização das relações contratuais demonstrou que os dados pessoais ocupam hoje uma posição central na economia digital. Mesmo quando o consumidor não paga em dinheiro, pode existir uma relação de valor económico sustentada na recolha e tratamento de dados pessoais. Essa realidade exige respostas jurídicas articuladas, capazes de proteger simultaneamente o consumidor e o titular dos dados.

O RGPD permanece o eixo estruturante da tutela dos dados pessoais, enquanto direito fundamental. As Diretivas (UE) 2019/770 e 2019/771, bem como a sua transposição para o ordenamento jurídico português pelo Decreto-Lei n.º 84/2021, vieram reforçar a tutela contratual dos consumidores em ambiente digital. O desafio atual consiste em aplicar estes regimes de forma coerente, evitando tanto a mercantilização acrítica dos dados pessoais como a ilusão de que serviços digitais "gratuitos" não envolvem verdadeiras contrapartidas.

A proteção jurídica dos dados pessoais, face à digitalização, exige assim mais do que normas isoladas. Exige transparência, responsabilidade, literacia digital, supervisão efetiva e uma compreensão rigorosa da dupla dimensão dos dados pessoais: valor económico na economia digital, mas, acima de tudo, expressão de um direito fundamental da pessoa.

Anaís de Menezes Leitão

Advogada estagiária

Teixeira Advogados & Associados

Notas

[1] OCDE, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 2013; Miguel Narciso, "*Dados Pessoais como Contraprestação em Contratos de Consumo - Breve Reflexão*", in Jorge Morais Carvalho (coord.), Anuário do Nova Consumer Lab - Yearbook of the Nova Consumer Lab, Ano 3, Nova Consumer Lab, 2021.

[2] European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 2017.

[3] Acórdão do Consiglio di Stato, Secção VI, 29 de março de 2021, referido na doutrina sobre dados pessoais como contrapartida e proteção do consumidor.

[4] A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, 2017.

Contacto profissional

Teixeira Advogados & Associados, Sociedade de Responsabilidade Limitada

Aveiro | Porto (Maia) | Lisboa

R. Conselheiro Luís de Magalhães, n.º 46, 1.º B1 | R. Dr. Augusto Martins, n.º 90, 2.º andar, sala 6 | Av. Fontes Pereira de Melo, n.º 16, IDEA Spaces

(+351) 234 428 503 | (+351) 919 044 909 | geral@teixeira-advogados.com

DPO MAGAZINE n.º 11

Setores Específicos

A Proteção de Dados Pessoais na Indústria Musical: Overview e desafios

David Serras Pereira

Introdução

A indústria musical contemporânea é marcada por uma intensa circulação de informação, quer no plano criativo, quer no plano comercial. Para além da gestão dos direitos de autor e direitos conexos, que historicamente constituíram o núcleo jurídico das relações contratuais no setor, emerge hoje a necessidade de assegurar a conformidade com as normas de proteção de dados pessoais. O Regulamento Geral sobre a Proteção de Dados (RGPD) e a Lei n.º 58/2019, que assegura a execução do mesmo no ordenamento jurídico português, impõem um conjunto de obrigações que não podem ser ignoradas pelos agentes culturais, editoras, entidades de gestão coletiva, produtores fonográficos e artísticos, bem como pelas plataformas de distribuição digital.

Enquadramento jurídico

Os contratos utilizados na indústria musical — contratos de edição, de gestão editorial, de artista, de sincronização ou de distribuição digital — implicam inevitavelmente o tratamento de dados pessoais. Para além do nome civil ou artístico, incluem-se dados de identificação fiscal, dados bancários, contactos, afiliações a entidades de gestão coletiva e informação relativa a remunerações, adiantamentos ou royalties. Em determinados contextos podem ainda ser tratados dados qualificados como sensíveis, como sucede com informações de saúde constantes de riders técnicos em digressões, ou dados reveladores de filiação sindical no caso de músicos de orquestra.

Todo este tratamento deve assentar numa base de licitude válida, como a execução do contrato, o cumprimento de obrigação legal ou, em determinadas situações, o consentimento do titular. A omissão desta análise prévia compromete a validade do tratamento e pode gerar responsabilidade contraordenacional, bem como responsabilidade civil nos termos gerais.

As cláusulas contratuais como instrumento de conformidade

Embora nem sempre expressamente contempladas, as cláusulas contratuais relativas à proteção de dados assumem hoje um papel determinante. É recomendável que cada contrato identifique, de forma clara, qual das partes atua como responsável pelo tratamento e qual poderá intervir na qualidade de subcontratante. Devem ser igualmente especificadas as finalidades do tratamento, os prazos de conservação e as medidas técnicas e organizativas implementadas para garantir a confidencialidade e a integridade da informação.

A circulação de dados no setor musical não se limita às partes do contrato. A realidade demonstra que os dados de autores e artistas são frequentemente transmitidos a terceiros, incluindo sociedades de gestão coletiva, plataformas digitais como Spotify, Apple Music ou YouTube, promotores de espetáculos e parceiros de comunicação. Tal transmissão deve ser objeto de previsão contratual e sujeita ao princípio da transparência, garantindo ao titular a devida informação sobre as entidades que acedem aos seus dados.

Importa ainda salientar a dimensão transnacional do mercado musical. A exploração de obras e fonogramas implica, em regra, a transferência de dados para fora do Espaço Económico Europeu. Nessas situações, os contratos devem prever a adoção de instrumentos jurídicos adequados, como as cláusulas contratuais-tipo aprovadas pela Comissão Europeia, ou a verificação da existência de decisão de adequação.

Os direitos dos titulares de dados no contexto musical

Os artistas e autores, para além de titulares de direitos de propriedade intelectual, são igualmente titulares de dados pessoais, beneficiando de um conjunto de direitos que lhes permite controlar e acompanhar a forma como os seus dados são tratados. O direito de acesso permite-lhes conhecer quais os dados tratados pela sua editora ou distribuidora; o direito de portabilidade revela-se especialmente relevante em casos de mudança de entidade gestora, possibilitando a transmissão estruturada de catálogos, metadados e ficheiros; já o direito ao apagamento levanta complexas questões de compatibilização, na medida em que pode colidir com obrigações legais de conservação de registos contabilísticos ou com a necessidade de manter a integridade de bases de dados de repertório.

Também o direito de oposição assume relevância prática no setor, designadamente quanto ao envio de comunicações de marketing ou à utilização secundária de dados não estritamente necessários à execução do contrato.

Riscos e desafios específicos

O ecossistema digital acentuou os riscos de incumprimento. Os ficheiros de metadados musicais, ao integrarem por vezes informações excessivas (como números fiscais ou moradas), podem violar o princípio da minimização. Por sua vez, os eventos ao vivo introduzem novas problemáticas, como a utilização de tecnologias de bilhética eletrónica com reconhecimento facial, que suscitam dúvidas de proporcionalidade e de compatibilidade com as exigências legais aplicáveis a categorias especiais de dados, incluindo a eventual necessidade de avaliação de impacto.

Conclusão

A proteção de dados pessoais deixou de constituir uma preocupação periférica para se tornar elemento central no regime jurídico da indústria musical. O cumprimento do RGPD e da Lei n.º 58/2019 exige não apenas a adoção de medidas técnicas internas, mas também a integração explícita de cláusulas de proteção de dados nos contratos musicais, clarificando responsabilidades, direitos e deveres das partes.

Num setor cuja sobrevivência depende da confiança entre autores, intérpretes, produtores e entidades de gestão, a conformidade com a legislação de proteção de dados é hoje fator de credibilidade e de sustentabilidade. A articulação entre direitos de autor e direitos fundamentais à privacidade constitui, em suma, um desafio incontornável e uma oportunidade para afirmar uma cultura jurídica mais responsável e transparente.

DPO MAGAZINE n.º 11

Chamada de artigos

A DPO Magazine acolhe contributos técnicos, ensaios e reflexões sobre proteção de dados, privacidade, segurança da informação e governação digital.

Contribuir para a DPO Magazine é participar no debate qualificado sobre a maturidade da proteção de dados em Portugal.

Envio de contributos através dos canais editoriais da APDPO.

JAVALI
OPEN SOURCE SYSTEMS

A solução web à medida do seu negócio

+ 20 anos experiência

+ 300 clientes satisfeitos

+ 10 setores de atividade

+ 300 projetos desenvolvidos

Serviços e soluções para projetos de sucesso

- Consultoria
- Gestão de Projeto
- Web Design
- Desenvolvimento web - Drupal
- Formação
- Suporte pós-produção
- Manutenção
- Websites
- Intranets
- Lojas online
- Plataformas para Instituições de Ensino
- Plataforma para Rent-a-Car
- Desenvolvimento à medida

MINISTÉRIO PÚBLICO
PORTUGAL

"Vimos por este meio expressar o gosto que tivemos em trabalhar com a Javali, foi extremamente gratificante, em grande parte pela sintonia e perfeita colaboração com a PGR, mas também, e sobretudo, pela extrema simpatia da vossa equipa, disponibilidade, profissionalismo e competência."

Nelson Coelho e Cândida Ferreira, Procuradoria-Geral da República

CASCAIS
Tudo começa nas pessoas

"Quando a Câmara Municipal de Cascais apostou na criação do seu novo portal, a Javali foi a empresa escolhida para a sua implementação. De lá para cá têm sido nossos parceiros na manutenção técnica e evolutiva do portal, dando resposta na íntegra às necessidades de um projeto que sabemos inovador e criativo."

Matilde Cardoso, Câmara Municipal de Cascais

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

BANCO DE PORTUGAL
EUROSISTEMA

Secretaria-Geral da Educação e Ciência

DGES
Direção-Geral do Ensino Superior

UCCLA

GRUPO Manuel Champalimaud

sumol+compal
É da nossa natureza.

omi

Ispa

NOVA
FACULDADE DE CIÊNCIAS E TECNOLOGIA

NICE RENT

Oliveira Seguros

esop

Contacte-nos

(+351) 212 957 215 | info@javali.pt | www.javali.pt