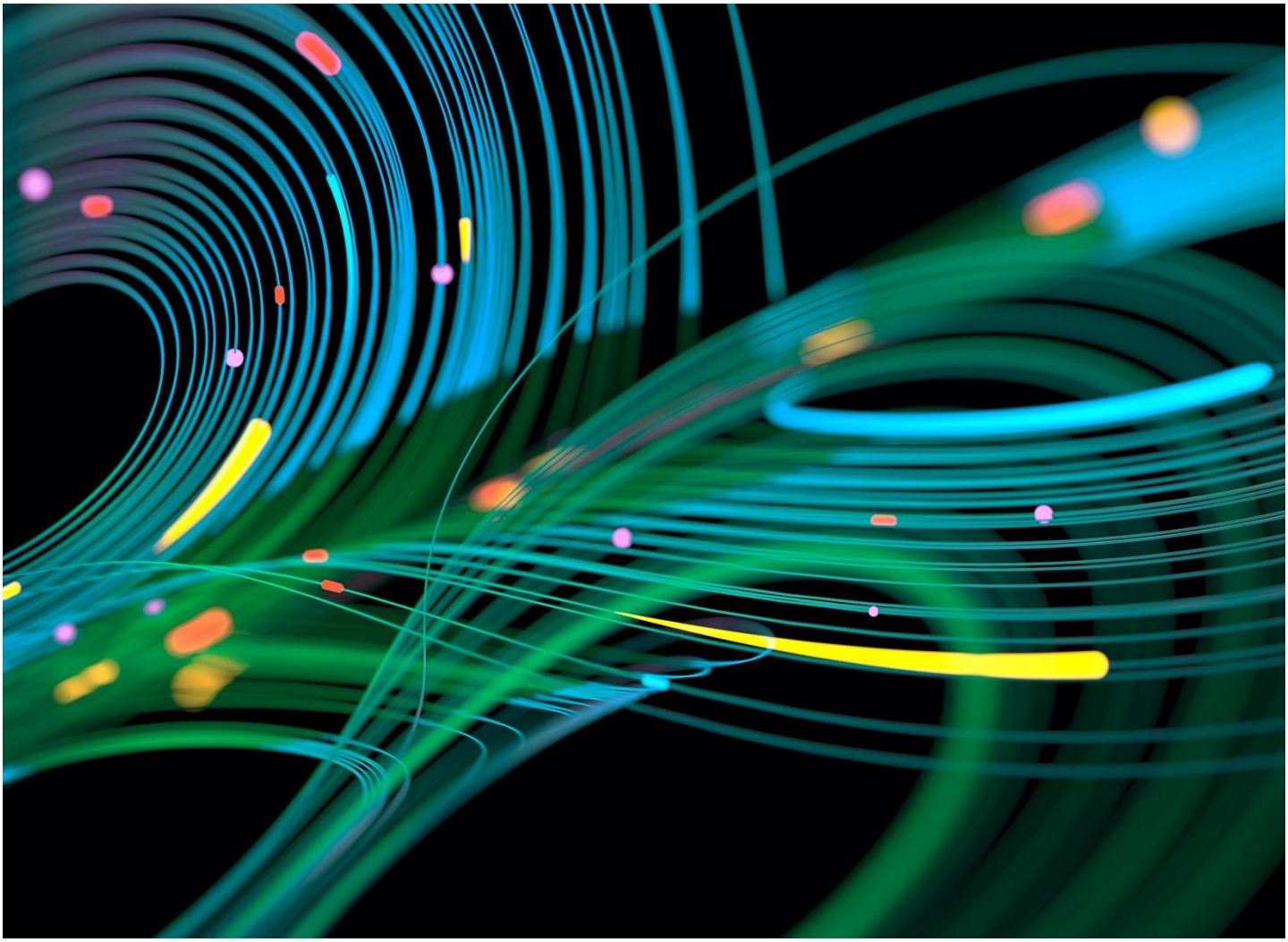
GARRIGUES

# Newsletter Economia de Dados, Privacidade e Cibersegurança

**Abril de 2026**

Últimas novidades de direito digital e inovação tecnológica, com decisões recentes e acórdãos relevantes sobre IA, *e-commerce* e regulamentação tecnológica



# O Supremo Tribunal estabelece o alcance do conceito de "tratamento" e obriga a cumprir os princípios do RGPD a partir do pedido de dados pessoais

Álvaro Blanco e Javier Enebral

**O Supremo Tribunal proferiu um acórdão histórico que fixa doutrina jurisprudencial em matéria de RGPD: o simples pedido de dados pessoais constitui "tratamento" de dados para efeitos do RGPD. A decisão resulta de um recurso interposto pela Agência Espanhola de Proteção de Dados (AEPD), representada pelo escritório de advogados Garrigues.**

A Secção de Contencioso Administrativo do Supremo Tribunal proferiu um acórdão particularmente relevante em 26 de março de 2026 (notificado em 21 de abril), na área da proteção de dados pessoais, uma vez que aborda, pela primeira vez em Espanha, o âmbito do conceito de "tratamento" de dados pessoais, tal como definido no artigo 4.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados (RGPD). A este respeito, o Supremo Tribunal declarou que o **responsável pelo tratamento de dados está sujeito ao cumprimento dos princípios que regem o tratamento de dados**, incluindo o princípio da minimização dos dados (artigo 5.º, n.º 1, alínea c), do RGPD), **desde o momento em que solicita dados pessoais a uma pessoa singular, independentemente de esses dados virem a ser efetivamente fornecidos** e posteriormente recolhidos pelo responsável pelo tratamento.

## Antecedentes do caso

O caso decorre de um processo sancionatório instaurado pela Agência Espanhola de Proteção de Dados (AEPD) contra a Secretaria-Geral das Instituições Penitenciárias (SGIIPP). Conforme consta dos factos assentes do acórdão, em 2019, um funcionário do Centro Penitenciário de Lanzarote ausentou-se do trabalho durante três dias por motivos de saúde, apresentando o respetivo atestado médico com a indicação de "indisposição". Justificou ainda uma ausência parcial posterior com um atestado que comprovava a sua presença numa consulta médica.

Após a apresentação destes documentos comprovativos, a Direção do Centro Penitenciário solicitou ao funcionário que fornecesse o diagnóstico médico específico e o tratamento prescrito. O funcionário

recusou-se a fornecer esta informação, alegando que se tratava de uma questão de privacidade pessoal e, por isso, desnecessária. Como consequência da sua recusa, foi sujeito a medidas disciplinares.

A AEPD, após a instrução do correspondente processo sancionatório, aplicou uma advertência à Secretaria-Geral das Instituições Penitenciárias por violação do princípio da minimização de dados estabelecido no Artigo 5.º, n.º 1, alínea c) do RGPD, considerando o pedido do diagnóstico médico excessivo e desnecessário para efeitos de controlo do absentismo laboral.

## Decisão da Audiência Nacional: a interpretação restritiva

Face à sanção imposta pela AEPD, a SGIIPP interpôs recurso administrativo para a Audiência Nacional. Este tribunal proferiu uma decisão inicial que anulava a sanção imposta pela AEPD, adotando uma interpretação formalista e literal do artigo 4.º, n.º 2 do RGPD e considerando que não poderia haver "tratamento" de dados se não tivesse havido efetivamente a sua recolha em qualquer momento. Na sua fundamentação, a Secção considerou que, uma vez que o funcionário não forneceu os dados solicitados, a Administração não podia iniciar qualquer tratamento e, por isso, não existia o elemento típico da infração ao princípio da minimização de dados pessoais.

## Recurso de cassação e a questão do interesse jurídico

A AEPD interpôs recurso de cassação contra a decisão da Audiência Nacional. A representação jurídica no caso foi assegurada, tal como na instância anterior, por profissionais da área de Economia de Dados, Privacidade e Cibersegurança da Garrigues.

A AEPD argumentou que a interpretação da Audiência Nacional era contrária à jurisprudência do Tribunal de Justiça da União Europeia (TJUE), citando, entre outras, os acórdãos de 24 de fevereiro de 2022 (Processo C-175/20), 5 de outubro de 2023 (Processo C-659/22) e 4 de outubro de 2024 (Processo C-548/21). O argumento do recurso centrou-se na premissa de que o RGPD exige que qualquer responsável pelo tratamento implemente os seus procedimentos de acordo com os princípios estabelecidos no RGPD a priori e antes do tratamento físico de quaisquer dados pessoais. Por conseguinte, a conformidade com o RGPD, incluindo o princípio da minimização de dados, deve ocorrer antes de os dados serem fisicamente recebidos pelo responsável pelo tratamento dos dados, em conformidade com os princípios de *accountability* (responsabilidade proativa ou prestação de contas) e da privacidade desde a conceção.

## A doutrina estabelecida pelo Supremo Tribunal

No acórdão aqui analisado, o Supremo Tribunal anulou a sentença da Audiência Nacional, apresentando os seguintes argumentos e fixando a seguinte doutrina jurisprudencial:

- **Interpretação ampla e sistemática do artigo 4.º, n.º 2, do RGPD.** A Secção rejeitou a interpretação literal e formalista que condicionava a existência do "tratamento" à efetiva recolha de dados. Em vez disso, adota uma interpretação sistemática que liga a definição do artigo 4.º, n.º 2, às obrigações do responsável pelo tratamento de dados decorrentes dos artigos 5.º e 25.º do RGPD. O Tribunal conclui que o "tratamento de dados" já existe quando a Administração solicita dados pessoais a uma pessoa singular, mesmo que o titular dos dados não os forneça, em última instância, dada a natureza de *numerus apertus* da lista de atividades descritas no artigo 4.º, n.º 2, do RGPD como constitutivas de um tratamento de dados.

- **Proteção efetiva dos direitos fundamentais.** O Supremo Tribunal sublinha que a proteção efetiva dos direitos fundamentais reconhecidos no artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da UE e no artigo 18.º da Constituição espanhola só é possível se o tratamento de dados for considerado como iniciado no momento do pedido de fornecimento de dados pessoais. Condicionar o cumprimento dos princípios ao momento efetivo da receção física dos dados

prejudicaria a proteção dos direitos dos titulares dos dados e geraria incerteza incompatível com o princípio da segurança jurídica.

- **Alinhamento com a jurisprudência do TJUE** O acórdão do Supremo Tribunal alinha-se expressamente com a doutrina do TJUE, que, no seu acórdão de 24 de fevereiro de 2022 (Processo C-175/20), já declarou que o legislador da UE pretendia dar um "alcance amplo" ao conceito de tratamento, observando que um pedido de dados pessoais por uma administração pública implica um processo de recolha para efeitos do artigo 4.º, n.º 2, do RGPD. Invoca ainda o acórdão do Tribunal de Justiça da União Europeia de 5 de outubro de 2023 (Processo C-659/22), que reitera esta interpretação ampla.

## Aplicação ao caso concreto: violação do princípio de minimização

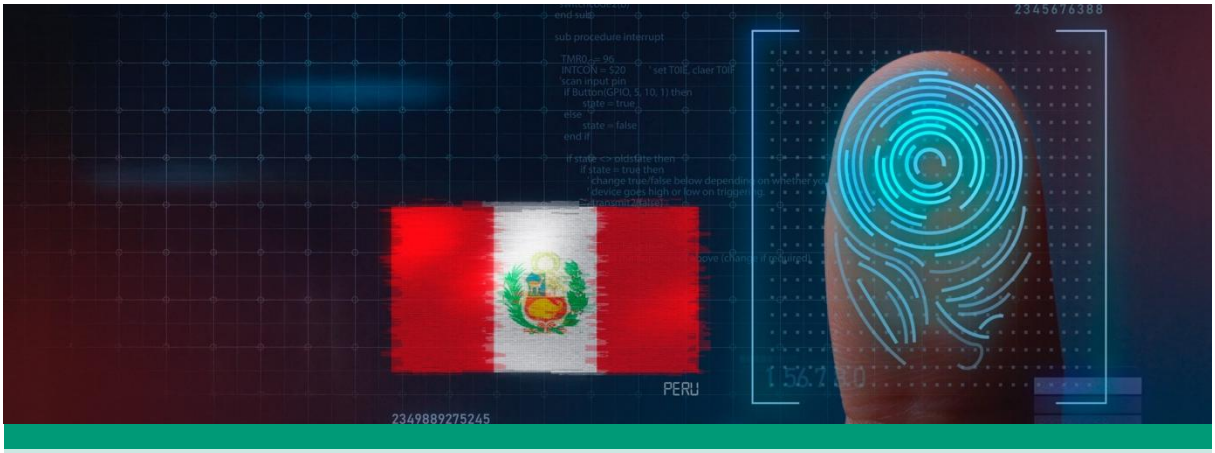
No caso em apreço, o Tribunal considerou que o Centro Penitenciário de Lanzarote **violou o princípio da minimização de dados ao solicitar o diagnóstico médico do funcionário, uma vez que essa informação não era adequada, pertinente ou necessária para o controlo do absentismo laboral**, que poderia ser exercido de forma satisfatória com os atestados médicos genéricos já fornecidos. O Tribunal sublinhou que se tratava de dados de saúde especialmente protegidos e que, mesmo em casos de baixa médica formal, centro de trabalho não tem, nem deveria ter, acesso ao diagnóstico médico do trabalhador, uma vez que tanto o Instituto Nacional de Segurança Social (INSS) como o Fundo Mútuo de Seguros da Função Pública (MUFACE) excluem expressamente esta informação dos relatórios submetidos ao empregador.

## Importância relevante do critério estabelecido

Esta decisão constitui um marco na interpretação do RGPD em Espanha por diversas razões. Em primeiro lugar, porque o Supremo Tribunal estabelece, pela primeira vez, o seu critério jurisprudencial sobre o âmbito do conceito de "tratamento" de dados pessoais até fases tão precoces como o próprio pedido, uma questão que não tinha sido abordada anteriormente em sede de cassação. Em segundo lugar, porque alinha a jurisprudência espanhola com a doutrina que o Tribunal de Justiça da União Europeia (TJUE) tem vindo a defender desde 2022 nas decisões acima referidas, reforçando a coerência do sistema de proteção de dados a nível europeu. E, em terceiro lugar, porque tem um impacto prático de longo alcance: qualquer entidade, pública ou privada, que atue como responsável pelo tratamento dos dados deve avaliar a conformidade com os princípios do RGPD, especialmente o da minimização, antes de fazer qualquer pedido de dados pessoais, e não apenas depois de os dados já terem sido recolhidos.

O critério fixado pelo Supremo Tribunal reforça a abordagem preventiva e proativa que inspira o RGPD, consolidando o princípio da responsabilidade proativa (*accountability*) e da proteção de dados desde a conceção e por defeito. Isto significa que as organizações são obrigadas a conceber os seus processos de recolha de dados de acordo com os princípios do regulamento antes de realizarem qualquer atividade de tratamento.

# Evolução da regulamentação de dados pessoais no Peru: implementação do novo regulamento, ações administrativas e projeções normativas




Franco Muschi e Mariana Ubidia

**A regulação dos dados pessoais no Peru evoluiu com particular dinamismo nos últimos anos. Este progresso deve-se tanto ao reforço do quadro normativo (gerado pela entrada em vigor do novo Regulamento da Lei de Protecção de Dados Pessoais) como à supervisão cada vez mais ativa e técnica da Autoridade Nacional para a Protecção de Dados Pessoais. Estas medidas visam consolidar e modernizar o sistema de proteção, reafirmando a proteção constitucional dos dados pessoais no Peru. O resultado é um ambiente regulatório que exige que as entidades públicas e privadas tratem os dados de forma mais responsável, segura e em conformidade com as normas internacionais em vigor.**

A seguir, apresentamos alguns dos avanços mais significativos nesta área.

## Quadro normativo em vigor

### Publicação do Novo Regulamento de Dados Pessoais

O novo Regulamento da Lei de Proteção de Dados Pessoais foi publicado a 30 de novembro de 2024 (Decreto Supremo n.º 016-2024-JUS). Este regulamento entrou em vigor a 30 de março de 2025, revogando o regulamento anterior, que estava em vigor desde 2013. As principais alterações introduzidas pelo regulamento são descritas a seguir:

1. **Notificação de incidentes de segurança**

   Estabelece a obrigação de notificar a Autoridade de Proteção de Dados Pessoais no prazo de 48 horas após o conhecimento de um incidente de segurança. Além disso, se o incidente afetar diretamente o titular dos dados, este também deverá ser notificado dentro do mesmo prazo.

   Se o incidente tiver sido resolvido internamente, sem afetar os dados pessoais, a notificação será feita exclusivamente à Autoridade de Proteção de Dados Pessoais.

De igual modo, o Centro Nacional de Segurança Digital deverá ser notificado quando o incidente de segurança ocorrer no e/ou através do ambiente digital.

Esta obrigatoriedade é de grande importância, pois, durante o primeiro semestre de 2025, foram registadas mais de 748 milhões de tentativas de ciberataques em todo o país.

2. **Nomeação de um Encarregado da Proteção de Dados**

As entidades públicas e privadas que lidam com grandes volumes de dados pessoais, que podem ter impacto num número significativo de pessoas, ou que realizam atividades comerciais essenciais ou relacionadas que envolvam o tratamento de dados sensíveis, são obrigadas a nomear um Encarregado da Proteção de Dados (EPD).

Esta nomeação deve ser formalizada internamente através de uma deliberação da Direção e comunicada à Autoridade de Proteção de Dados. Além disso, as informações de contacto do Encarregado da Proteção de Dados devem ser divulgadas num local visível para os titulares dos dados dentro da empresa.

De referir que a Autoridade de Proteção de Dados emitiu as disposições para a nomeação do EPD no final de 2025, incluindo requisitos legais relacionados com o perfil, experiência e formação do EPD, além de outros elementos importantes para determinar a aplicabilidade desta obrigação.

A Autoridade concedeu um prazo adicional para adaptação a estas novas disposições até junho de 2026.

3. **Simplificação do Registo de Bases de Dados Pessoais**

O processo de registo, modificação ou cancelamento de bases de dados pessoais junto da Autoridade de Proteção de Dados Pessoais foi simplificado. Consequentemente, tornou-se um procedimento de aprovação automática sujeito a fiscalização sucessiva.

## Publicação da metodologia para o cálculo de coimas em matéria de proteção de dados pessoais

A 31 de dezembro de 2025, foi publicada a metodologia para o cálculo de coimas em matéria de proteção de dados pessoais. O seu objetivo é estabelecer um método claro e objetivo para o cálculo das coimas por violações das normas de proteção de dados pessoais, já que atualmente são calculadas utilizando intervalos demasiado amplos para uma determinação objetiva. A seguir, a título de exemplo, são apresentadas algumas modificações com base nas novas violações incluídas nas novas normas:

| Infração | Valor proposto pelo projeto |
|---|---|
| Falta de comunicação do fluxo de dados transfronteiriços. | 1.08 UIT |
| Tratamento de dados pessoais com violação das medidas de segurança estabelecidas, causando danos ao titular dos dados ou expondo os seus dados sem a sua autorização. | 7.50 – 37.50 UIT |
| Tratamento de dados pessoais sensíveis com violação das medidas de segurança estabelecidas, causando Sensível danos ao titular dos dados ou expondo os seus dados sem a sua autorização. | 73.33 UIT |

Foram também estabelecidas as seguintes alterações:

| Metodologia para o cálculo publicado em 2020 | Projeto de metodologia para o cálculo proposto |
|---|---|
| Será aplicado um agravamento de 20% a quem praticar uma infração que gere risco ou dano a mais de **duas pessoas ou grupo** de pessoas. | Será aplicado um agravamento de 20% a quem praticar uma infração que gere risco ou dano a mais de **uma** pessoa ou grupo de pessoas. |
| Será aplicada uma redução de 30% a quem reconhecer a responsabilidade de forma expressa e por escrito pelas acusações, **depois de ter sido notificada do início do procedimento sancionatório**. | Será aplicada uma redução de 30% a quem reconhecer a responsabilidade de forma expressa e por escrito pelas acusações, até **antes do relatório final de investigação**. |

## Atuação da Autoridade de Proteção de Dados Pessoais: o que ocorreu em 2025

### Sanções e tendências nos setores fiscalizados

De acordo com a Autoridade de Proteção de Dados Pessoais, o número de sanções impostas pelo tratamento inadequado de informações pessoais aumentou. A seguir, apresentamos os dados mais relevantes no final de 2025:

- 11,3 milhões de soles em coimas por violações da legislação em vigor.
- 760 entidades públicas e privadas foram fiscalizadas, principalmente nos setores financeiro e das telecomunicações.
- 198 visitas de inspeção em todo o país.
- 136 novos procedimentos sancionatórios administrativos.
- 211 resoluções administrativas em primeira e segunda instâncias.

### Pronunciamentos relevantes: critérios da Autoridade Nacional para a Proteção de Dados Pessoais

Os pareceres consultivos emitidos pela Autoridade Nacional para a Proteção de Dados Pessoais são pronunciamentos técnicos não vinculativos que interpretam e clarificam o âmbito da Lei de Proteção de Dados Pessoais e dos seus regulamentos, oferecendo critérios para orientar as entidades públicas e privadas no cumprimento das suas obrigações. Neste contexto, apresentamos de seguida os três critérios mais relevantes emitidos pela ANPD:

#### Quem é o responsável pelo tratamento de dados nos serviços públicos concessionados? (Parecer Consultivo n.º 001-2026-DGTAIPD de fevereiro de 2026)

Confirma-se que a empresa concessionária, que determina as finalidades, os meios e as medidas de segurança do tratamento, é responsável pelo tratamento dos dados pessoais dos utilizadores nos serviços públicos oferecidos por ela. Neste sentido, qualquer terceiro encarregado de uma operação específica (por exemplo, videovigilância ou serviços de suporte) atua como responsável pelo tratamento de dados ou, se subcontratado pelo responsável pelo tratamento de dados, como subcontratante.

Além disso, esclarece-se que qualquer fornecimento de dados constitui uma transferência, que só é válida se expressamente autorizada pelo titular dos dados. A finalidade, os prazos e as obrigações, assim como as medidas de segurança e rastreabilidade que impeçam utilizações ou subtransmissões para fins diferentes dos instruídos, devem ser documentadas contratualmente.

**As reuniões da direção de uma pessoa coletiva podem ser gravadas? (Parecer Consultivo n.º 037-2025-JUS/DGTAIPD de setembro de 2025)**

Este Parecer estabelece que a voz de uma pessoa é considerada um dado pessoal que deve ser analisado sob duas perspetivas: (i) a informação transmitida através da mesma e (ii) as características físicas associadas ao titular dos dados. No que diz respeito às gravações áudio das reuniões da direção de uma pessoa coletiva, se estas estiverem reguladas nos estatutos da entidade, não é necessário obter o consentimento dos participantes (diretores) para a sua gravação, desde que sejam discutidos assuntos relacionados com a pessoa coletiva, uma vez que a pessoa estaria a atuar em seu nome.

Uma vez cumprida a finalidade da gravação de uma reunião da direção, qualquer tratamento subsequente dos dados gravados se enquadra no âmbito da Lei de Proteção de Dados Pessoais, já que excede a finalidade original de representação da entidade. O titular dos dados pessoais tem o direito de se opor ao tratamento e de solicitar o apagamento dos seus dados, o que exigirá uma avaliação específica de cada caso na instância administrativa competente.

**Como garantir a exatidão dos dados pessoais no tratamento de informações laborais? (Parecer Consultivo n.º 013-2025-JUS/DGTAIPD de março de 2025)**

O Parecer estabelece que os dados contidos em fontes publicamente acessíveis devem ser utilizados exclusivamente para os fins para os quais foram criados e disponibilizados. Caso seja necessário utilizar estes dados para outros fins, deverá ser obtido o consentimento do titular dos dados. Os empregadores ou potenciais empregadores podem utilizar informações públicas, como notícias ou registos públicos, para verificar a exatidão dos dados fornecidos pelos candidatos ou colaboradores sem o seu consentimento, desde que respeitem os princípios da Lei de Proteção de Dados Pessoais (LPDP).

Reafirma ainda que apenas as autoridades legalmente autorizadas podem tratar dados pessoais relacionados com infrações penais ou contraordenacionais. Qualquer outra pessoa ou entidade que pretenda aceder a esta informação deverá obter o consentimento prévio, livre e informado do titular dos dados. No caso de registos criminais, policiais ou judiciais, as informações devem ser solicitadas diretamente ao titular dos dados.

## Agenda 2026

### Caso relevante

O início de 2026 confirma que o setor bancário e financeiro continuará a ser um alvo relevante para a Autoridade Nacional de Proteção de Dados Pessoais.

Neste sentido, no início do ano, três bancos foram sancionados por recolher, armazenar e utilizar impressões digitais e dados biométricos de clientes e não clientes sem consentimento ou notificação prévia. Verificou-se que estes bancos, apesar de terem acesso ao serviço de verificação biométrica do Registo Nacional de Identificação e Estado Civil (RENIEC), também armazenavam os dados biométricos nas suas próprias bases de dados.

Num dos casos, uma instituição financeira foi sancionada em 24,75 UIT (S/ 122.512,50) por armazenar as impressões digitais de uma pessoa sem vínculo contratual com a instituição, que apenas a visitou para efetuar um depósito. Embora a instituição utilizasse o serviço de verificação biométrica do RENIEC, também retinha as impressões digitais nos seus próprios sistemas. A sanção foi mantida em sede de recurso.

No segundo caso, um outro banco foi sancionado em 66 UIT (S/ 326.700,00) depois de se ter verificado que recolhia impressões digitais de clientes e não clientes sob o pretexto de validação junto do RENIEC, mas armazenava os dados biométricos para utilização adicional sem informar os titulares dos dados.

Em ambos os casos, foram impostas coimas adicionais de 4,89 UIT e 13,50 UIT, respetivamente, pela ausência de políticas de privacidade claras, abrangentes e prévias relativas ao tratamento de dados biométricos.

Por fim, uma outra instituição financeira foi multada em 7,5 UIT (S/ 37.125,00) por deficiências nas medidas de segurança que comprometeram a confidencialidade e a integridade da informação biométrica dos utilizadores.

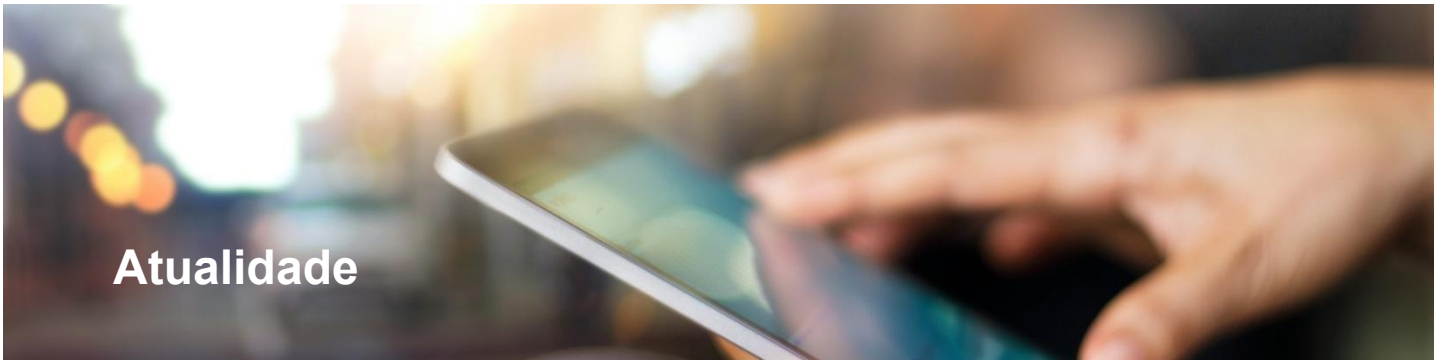
## Dados Pessoais na Administração Pública para 2026: Estratégia Nacional de Governação de Dados

Em resposta à digitalização e transformação digital em curso, foi proposta a Estratégia Nacional de Governação de Dados (ENGD). O seu objetivo é melhorar a gestão de dados públicos no Peru, promovendo a sua utilização eficiente, acessível e segura na administração pública.

Esta estratégia centra-se na governação de dados e na criação de plataformas interligadas, como a DATOS PERÚ, o Centro Nacional de Dados e a Plataforma Nacional de Dados Abertos, que facilitam a troca de informação entre entidades públicas. Além disso, promove a utilização de tecnologias, como a análise de dados e a inteligência artificial, para otimizar a tomada de decisões e prestar melhores serviços.

Esta estratégia envolve o setor privado, promovendo a reutilização eficiente em termos de custo de dados públicos, fomentando desafios de inovação e programas de apoio empresarial e garantindo o acesso a dados padronizados. Complementarmente, propõe a interoperabilidade alinhada com as normas da OCDE, facilitando a troca segura de dados entre o Estado e as empresas. ¡

Além disso, a estratégia exige a construção de espaços de dados seguros, em que o setor privado participe em conjunto com o Estado através de serviços de interoperabilidade e segurança. Exige também consultas regulares às empresas para orientar os planos de dados abertos e apoiar iniciativas privadas que utilizem dados públicos para abordar questões de políticas públicas.



# Atualidade

## Parecer conjunto do Comité Europeu para a Proteção de Dados e da Autoridade Europeia de Proteção de Dados sobre a proposta de regulamento digital Omnibus para simplificar o quadro regulamentar europeu

O Comité Europeu para a Proteção de Dados (CEPD) e o Autoridade Europeia para a Proteção de Dados (AEPD) emitiram um parecer conjunto em resposta à proposta de regulamento intitulada "Omnibus Digital", apresentada pela Comissão Europeia em 19 de novembro de 2025. Esta proposta legislativa visa alterar um vasto leque de normas da União Europeia em matéria digital, incluindo o RGPD, a Diretiva *ePrivacy*, o Regulamento de Dados e a Diretiva NIS 2, com o objetivo de simplificar o quadro regulamentar digital da União Europeia, reduzir a carga administrativa e melhorar a competitividade das organizações europeias.

Assim, o CEPD e o AEPD avaliam se a proposta (i) conduz a uma simplificação genuína e facilita o cumprimento da regulamentação, (ii) proporciona maior segurança jurídica e (iii) afeta os direitos humanos fundamentais.

Neste sentido, o documento está estruturado em secções que analisam as alterações propostas relativamente a cada legislação afetada, formulando recomendações específicas em cada área. Por conseguinte, embora acolham favoravelmente os objetivos de simplificação prosseguidos pelo Digital Omnibus, o CEPD e a AEPD alertam para a necessidade de garantir que estas simplificações não comprometem o elevado nível de proteção dos direitos e liberdades fundamentais das pessoas singulares. Lamentam ainda que a proposta não tenha sido acompanhada de uma avaliação de impacto completa.

A este respeito, entre as modificações mais relevantes contidas no Digital Omnibus e abordadas no parecer, destacam-se a alteração da definição de dados pessoais (sobre a qual ambas as autoridades manifestam sérias reservas), a introdução de uma definição de investigação científica, novas exceções para o tratamento de dados biométricos, a utilização do interesse legítimo no contexto da inteligência artificial, alterações relativas aos direitos dos titulares dos dados (acesso, transparência e tomada de decisões automatizadas), o regime de notificação de violação de dados, as avaliações de impacto sobre a proteção de dados, a proteção de equipamentos terminais e *cookies*, e diversas disposições relativas à governação e reutilização de dados.

## O Conselho de Ministros aprovou o anteprojeto de nova Lei Orgânica sobre o direito à honra, à reserva da vida privada pessoal e familiar e à própria imagem.

O Conselho de Ministros aprovou o texto do anteprojeto de Lei Orgânica sobre a protecção civil do direito à honra, à reserva da vida privada pessoal e familiar e à própria imagem. Este anteprojeto substitui o texto normativo original de 1982, adaptando-o ao ambiente digital (inteligência artificial, redes sociais, etc.) e alargando o nível de proteção destes direitos fundamentais.

O texto proposto fortalece o quadro de proteção contra o uso não autorizado de imagens, vozes e outros elementos identificadores, e aborda fenómenos emergentes como os *deepfakes*. O

anteprojeto esclarece ainda, no seu preâmbulo, que o facto de um cidadão partilhar as suas próprias fotografias ou vídeos numa rede social não autoriza terceiros a reutilizá-los noutros canais ou plataformas.

A legislação alarga também a proteção de grupos especialmente vulneráveis. No caso dos menores, a idade mínima para prestar um consentimento válido quanto à utilização da sua imagem é fixada nos 16 anos, embora, mesmo com consentimento, a divulgação seja considerada ilegítima se prejudicar a sua dignidade ou reputação. A proteção das vítimas de crime é também reforçada, proibindo o agressor de utilizar os factos em detrimento da vítima. Além disso, prevê-se a possibilidade de as pessoas falecidas deixarem instruções para impedir a utilização da sua imagem ou voz para fins comerciais.

O texto mantém as exceções já reconhecidas na versão atual da legislação ou pela jurisprudência, sobretudo no que respeita à liberdade de expressão e de informação. Entre estas, destaca-se a possibilidade de utilização de técnicas de inteligência artificial para fins criativos, satíricos ou ficcionais, quando estas envolvam figuras públicas, desde que a utilização desta tecnologia seja claramente identificada.

## Consulta pública do Regulamento de Execução do Regime Jurídico da Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) publicou o projeto de regulamento de execução do Decreto-Lei n.º 125/2025, de 4 de dezembro, que aprova o Regime Jurídico da Cibersegurança (RJC) e transpõe para a ordem jurídica portuguesa a Diretiva (UE) 2022/2555 (NIS 2).

O regulamento é aplicável às entidades essenciais, entidades importantes e entidades públicas relevantes, nos termos definidos no RJC, e vem densificar as obrigações já previstas naquele diploma, estabelecendo regras operacionais e instrumentos concretos de conformidade.

Destacamos, em seguida, os principais aspetos do projeto de Regulamento:

### Plataforma eletrónica

Um eixo central do regulamento é a criação de uma plataforma eletrónica gerida pelo CNCS, que funcionará como ponto único de registo, qualificação e comunicação entre as entidades abrangidas e as autoridades de cibersegurança. Esta plataforma será o canal obrigatório para o cumprimento de diversas obrigações previstas no RJC, designadamente: a autoidentificação e registo das entidades; a notificação da qualificação de entidades; a comunicação do relatório anual; a designação do responsável de cibersegurança e do ponto de contacto permanente; a notificação de incidentes de cibersegurança e a notificação voluntária de informações pertinentes; e as notificações eletrónicas realizadas pelas autoridades de cibersegurança às entidades.

### Quadro Nacional de Referência de Cibersegurança

O Quadro Nacional de Referência de Cibersegurança (QNRCS), constante do Anexo I ao projeto de regulamento, constitui o instrumento nacional de referência para a identificação das normas, padrões e boas práticas em matéria de gestão da cibersegurança e da segurança da informação. De acordo com o artigo 14.º, n.º 3, do RJC, será o instrumento de referência para a determinação das medidas de cibersegurança a adotar pelas entidades abrangidas.

Importa salientar que o QNRCS e a Matriz de Risco (Anexo II) não estão sujeitos à consulta pública, pelo que os contributos dos interessados se limitarão ao articulado do regulamento e às medidas constantes dos Anexos III e IV.

### Matriz de risco e medidas de cibersegurança mínimas

O regulamento procede à definição de medidas de cibersegurança mínimas, associadas a três níveis de conformidade - "Básico", "Substancial" e "Elevado" - determinados por uma matriz de risco setorial. A Matriz de Risco, constante do Anexo II, pondera, para cada setor e subsetor, a probabilidade e o impacto de cenários de risco dominantes, tendo em conta a dimensão da entidade ("Grande", "Média" ou "Pequena") e a importância do setor (setores de importância crítica do Anexo I do

RJC ou outros setores críticos do Anexo II do mesmo diploma).

Os níveis de conformidade são cumulativos, pelo que as entidades sujeitas ao nível "Elevado" devem cumprir também as medidas previstas para os níveis "Básico" e "Substancial". As medidas de cibersegurança mínimas encontram-se densificadas no Anexo III (aplicável a entidades essenciais e importantes) e no Anexo IV (aplicável a entidades públicas relevantes, organizadas em Grupo A e Grupo B), abrangendo domínios como políticas de cibersegurança, inventário de ativos, gestão de risco e vulnerabilidades, gestão de acessos e autenticação multifator, proteção de equipamentos e redes, cópias de segurança, resposta a incidentes e gestão da cadeia de abastecimento.

### Próximos passos e implicações práticas

O projeto de regulamento esteve em consulta pública até ao 16 de abril de 2026, com exceção das disposições relativas ao QNRCS (Anexo I) e à matriz de risco (Anexo II). Neste momento, o CNCS encontra-se em fase de apreciação dos respetivos contributos apresentados, sendo que em seguida divulgará um relatório com um resumo desses contributos, bem como uma apreciação global sobre os mesmos e os fundamentos das opções tomadas na versão final do regulamento.

O regulamento entrará em vigor no quinto dia após a sua publicação, sem prejuízo das disposições transitórias previstas no Decreto-Lei n.º 125/2025.

O regulamento de execução do RJC constitui um instrumento fundamental para a concretização do quadro obrigacional em matéria de cibersegurança. As entidades abrangidas devem, desde já, iniciar a análise dos requisitos aplicáveis e preparar os respetivos processos internos, tendo em conta que algumas obrigações terão prazos de cumprimento curtos após a operacionalização da plataforma - designadamente, a autoidentificação das entidades, que deverá ocorrer no prazo de 60 dias.

## A AEPD publicou um guia sobre a utilização de imagens de terceiros em sistemas de inteligência artificial e os riscos associados.

Este documento analisa os riscos de carregar, transformar ou gerar conteúdo com IA utilizando imagens de pessoas, que podem ser divididos em riscos visíveis e invisíveis. O texto é particularmente útil para a realização de análises de risco de sistemas de inteligência artificial que processam imagens de terceiros.

Os riscos visíveis são aqueles que surgem quando o conteúdo gerado ou modificado é partilhado. Os principais fatores incluem a expectativa razoável de utilização da imagem pelo seu proprietário, a facilidade de disseminação nas redes sociais ou plataformas de mensagens, a dificuldade real de remoção de cópias e o potencial dano na reputação quando a imagem atribui eventos que nunca ocorreram. O documento destaca especificamente o elevado risco associado à geração de conteúdos íntimos ou sexualizados, à descontextualização de imagens e à utilização de imagens de pessoas vulneráveis, incluindo menores, idosos ou pessoas portadoras de deficiência.

Em segundo lugar, a AEPD especifica os riscos menos visíveis que resultam do mero carregamento de uma imagem para um sistema de inteligência artificial. Estes incluem, entre muitos outros, a perda de controlo sobre o ficheiro, o envolvimento de múltiplos agentes tecnológicos, a possibilidade de o fornecedor utilizar as imagens para outros fins e a geração automática de metadados. O documento alerta ainda para o risco de identificação persistente, a assimetria de informação que dificulta o exercício de direitos e a potencial exposição a incidentes de segurança.

## O Conselho Geral do Poder Judicial aprova uma instrução sobre o uso de inteligência artificial por juízes e magistrados

A 28 de janeiro de 2026, o Plenário do Conselho Geral do Poder Judicial (CGPJ) aprovou a Instrução 2/2026, sobre a utilização de sistemas de inteligência artificial no exercício da atividade jurisdicional, publicada

no Diário Oficial do Estado (BOE) de 30 de janeiro. O seu objetivo é estabelecer critérios, diretrizes de utilização e princípios para a utilização de sistemas de inteligência artificial (IA) por juízes e magistrados como ferramenta de apoio, garantindo a independência judicial e os direitos fundamentais, em conformidade com o Regulamento (UE) 2024/1689 sobre Inteligência Artificial (Regulamento de IA).

A instrução estabelece nove princípios: controlo humano efetivo, não substituição do juiz, plena responsabilidade judicial, independência judicial, respeito pelos direitos fundamentais, confidencialidade e segurança, prevenção do enviesamento algorítmico e proporcionalidade e formação contínua. O uso de IA é permitido para pesquisas de informação jurídica, análise e classificação de documentos, criação de esboços ou minutas internas e tarefas organizacionais. No entanto, é proibido utilizar a IA para substituir a tomada de decisões judiciais, integrar conteúdos sem validação crítica ou tratar dados especialmente protegidos fora das circunstâncias legalmente autorizadas. Apenas podem ser utilizados sistemas fornecidos pelas autoridades competentes ou pelo Conselho Geral do Poder Judicial (CGPJ); são proibidos sistemas externos, exceto para pesquisa de código aberto.

As minutas de decisões geradas pela IA exigem uma revisão e validação crítica pelo juiz ou magistrado antes de serem validadas como decisão judicial ou processual e não constituem decisões automatizadas.

O CGPJ supervisionará a utilização destes sistemas no que diz respeito ao tratamento de dados pessoais para fins jurisdicionais e oferecerá formação especializada. O não cumprimento da presente instrução poderá acarretar responsabilidade nos termos da Lei Orgânica 6/1985, de 1 de Julho, sobre o Poder Judicial.

## O Conselho para a Transparência e Proteção de Dados da Andaluzia analisa um sistema de IA para a seleção de pessoal

O Conselho para a Transparência e Proteção de Dados da Andaluzia publicou um documento técnico que analisa a utilização de sistemas de inteligência artificial para a avaliação de competências profissionais em processos de seleção de pessoal, especialmente no setor público.

O relatório aborda, numa perspetiva prática, as principais implicações da utilização de ferramentas automatizadas para a avaliação de candidatos, centrando-se em questões como a determinação do fundamento jurídico para o tratamento de dados, a possível aplicação do artigo 22.º do RGPD, relativo à tomada de decisões individuais automatizadas, e a necessidade de realizar uma avaliação de impacto sobre a proteção de dados (AIPD) quando o sistema possa gerar riscos significativos para os direitos e liberdades dos candidatos.

O documento sublinha que, quando um sistema de IA desempenha um papel decisivo na pré-seleção ou classificação dos candidatos, pode constituir uma decisão automatizada com efeitos legais ou significativamente semelhantes, exigindo garantias adicionais, incluindo o direito à intervenção humana e à contestação da decisão. Analisa também os requisitos de transparência, minimização de dados e técnicas de anonimização ou pseudonimização que poderiam ser aplicadas nas fases iniciais do processo.

O Conselho sublinha ainda a necessidade de documentar adequadamente o funcionamento do algoritmo e garantir que não ocorre qualquer viés discriminatório, reiterando que a responsabilidade proativa exige a demonstração da conformidade regulamentar antes da implementação do sistema.

## O Comité Europeu para a Proteção de Dados alerta a Comissão Europeia para o facto de as novas propostas de alteração do sistema ESTA implicarem uma recolha desproporcionada de dados de viajantes europeus

O Conselho Europeu para a Proteção de Dados (EDPB) manifestou a sua preocupação, numa carta dirigida à Comissão Europeia, relativamente às propostas dos Estados Unidos para modificar o processo de candidatura ao sistema eletrónico de autorização de viagem (ESTA), que permite aos cidadãos do Espaço

Económico Europeu entrar nos Estados Unidos sem visto para estadias inferiores a 90 dias.

Segundo o CEPD, as alterações propostas representam uma mudança substancial e problemática no tratamento de dados pessoais de cidadãos do EEE, uma vez que envolvem a recolha de um volume significativamente maior de informações, incluindo dados particularmente sensíveis, como a atividade nas redes sociais nos últimos cinco anos, informações sobre familiares não relacionadas com viagens e, potencialmente, até dados biométricos. O Comité sublinha que esta expansão é desproporcionada e não satisfaz uma necessidade comprovada.

Alerta ainda que a intenção de exigir que os pedidos sejam submetidos exclusivamente através da aplicação móvel ESTA reduz a acessibilidade e suscita preocupações quanto à transparência e segurança do sistema, especialmente porque não são indicados mecanismos eficazes para os titulares dos dados exercerem os seus direitos de proteção de dados. O Comité observa ainda que as propostas não esclarecem os períodos de conservação nem as condições em que os dados serão armazenados ou utilizados, o que agrava a falta de garantias disponíveis para os cidadãos europeus e cria incerteza quanto ao respeito pelos seus direitos fundamentais.

## O CEPD publica os resultados da consulta pública sobre modelos úteis para facilitar o cumprimento do RGPD pelas organizações

O Comité Europeu para a Proteção de Dados (CEPD) publicou um relatório sobre os resultados da consulta pública lançada entre 5 de novembro e 3 de dezembro de 2025, em que recolheu opiniões sobre modelos que poderiam facilitar as atividades de cumprimento do RGPD pelas organizações. A consulta, dirigida particularmente às PME e enquadrada nos compromissos assumidos na Declaração de Helsínquia para melhorar a clareza, o apoio e a participação das partes interessadas, recebeu um total de 82 contributos de associações empresariais, encarregados da proteção de dados, advogados, empresas, autoridades públicas, ONG, instituições académicas e particulares, 71 dos quais provenientes do EEE e 11 de países terceiros. Os modelos mais solicitados pelos contribuintes foram os relativos ao registo das atividades de tratamento (RAT), à avaliação do impacto na proteção de dados (AIPD), à avaliação do interesse legítimo, ao aviso ou política de privacidade, à avaliação do impacto das transferências, ao contrato de tratamento, ao formulário de notificação de violação de segurança e à avaliação do risco de privacidade.

Tendo em conta os contributos recebidos e considerando que o CEPD já tinha decidido trabalhar em modelos para avaliações de impacto na proteção de dados e notificações de violação de segurança, a Comissão integrou o desenvolvimento de três modelos adicionais no seu Programa de Trabalho 2026-2027: um modelo ou fluxograma para a avaliação do interesse legítimo, um para o registo das atividades de tratamento e outro para avisos ou políticas de privacidade. O CEPD desenvolverá estes modelos tendo em conta os já disponíveis a nível nacional e harmonizando-os, podendo considerar o desenvolvimento de modelos adicionais.

## Aprovado no Parlamento espanhol o primeiro regulamento sobre a utilização de inteligência artificial

A 16 de fevereiro de 2026, o Senado aprovou as Orientações para a Utilização da Inteligência Artificial no Senado, estabelecendo um quadro para a utilização responsável, ética e legal da IA. O seu objetivo é melhorar a eficiência parlamentar e administrativa, salvaguardando simultaneamente os direitos e as liberdades. Está em conformidade com o Regulamento (UE) 2024/1689 sobre Inteligência Artificial, o RGPD e a LOPDGDD, aplicando-se a senadores, funcionários, grupos parlamentares e estagiários. Identifica riscos para os direitos fundamentais (privacidade, parcialidade, propriedade intelectual), riscos operacionais, de segurança, de reputação e ambientais.

Os princípios orientadores incluem, entre outros: responsabilidade individual na utilização; fiabilidade, robustez e segurança dos sistemas; respeito pela autonomia humana; transparência; proporcionalidade e adequação às necessidades do Senado; supervisão humana obrigatória; responsabilização, incluindo a do prestador de serviços, quando aplicável; abertura e interoperabilidade;

privacidade; igualdade e não discriminação; e abertura ao avanço tecnológico.

No que diz respeito à aquisição e implementação de sistemas de IA, as diretrizes exigem principalmente: (i) uma avaliação prévia supervisionada pela Comissão de Segurança da Informação do Senado, (ii) uma avaliação de impacto, quando apropriado, (iii) documentação técnica detalhada e (iv) uma garantia do fornecedor do sistema de que a informação não pública introduzida no sistema não será utilizada para treinar qualquer modelo.

A Direção de Tecnologias da Informação e Comunicação é responsável pelo cumprimento, em coordenação com o responsável pela proteção de dados. Existem medidas disciplinares para o incumprimento. As orientações entram em vigor 60 dias após a sua publicação no Boletim Oficial do Estado (BOE) e permitem um período de adaptação de seis meses.

## A Comissão Europeia abre dois procedimentos para ajudar a Google a cumprir as obrigações de interoperabilidade e troca de informações ao abrigo do Regulamento dos Mercados Digitais.

A Comissão Europeia iniciou dois procedimentos com o objetivo de esclarecer como é que a Google — designada como "controlador de acesso" ao abrigo do Regulamento dos Mercados Digitais (DMA) — se deve adaptar a este regulamento. Este regulamento estabelece obrigações específicas para as plataformas que atuam como intermediários essenciais entre os consumidores e as empresas, de forma a evitar práticas que possam limitar a concorrência ou criar barreiras à entrada.

O primeiro procedimento centra-se no sistema operativo para dispositivos móveis. A Comissão pretende esclarecer como garantir que outros programadores têm acesso livre e efetivo a funcionalidades essenciais do sistema, incluindo as baseadas em inteligência artificial, como os sistemas de geração de conteúdos utilizados pela própria plataforma. O objetivo é assegurar que os fornecedores de IA de terceiros possam inovar e competir em condições de igualdade.

O segundo procedimento aborda o serviço de pesquisa. O regulamento exige que os concorrentes tenham acesso justo e não discriminatório a determinados dados anonimizados relacionados com consultas, cliques e visualizações. A Comissão irá avaliar que informações devem ser incluídas, como devem ser anonimizadas e se os fornecedores de assistentes conversacionais ou sistemas de IA generativa podem utilizar estes dados para desenvolver alternativas viáveis.

A Comissão irá analisar estes aspetos nos próximos meses, enviar conclusões preliminares à Google e convidar terceiros a apresentar comentários. A instauração destes procedimentos não implica que tenha ocorrido uma infração, mas também não impede a Comissão de impor medidas ou sanções no futuro, caso se verifique uma violação.

## O Comité Europeu de Proteção de Dados e a Autoridade Europeia de Proteção de Dados emitem um parecer conjunto sobre a proposta de Ato Legislativo Europeu de Biotecnologia

O Conselho Europeu de Proteção de Dados (CEPD) e a Autoridade Europeia de Proteção de Dados (AEPD) adotaram um parecer conjunto sobre a proposta da Comissão Europeia para um Ato Legislativo de Biotecnologia, destinado a reforçar os setores da biotecnologia e da biofabricação na área da saúde. Ambas as instituições apoiam a criação de uma base jurídica única para o tratamento de dados pessoais por parte de patrocinadores e investigadores, mas alertam que a elevada sensibilidade dos dados genéticos e de saúde exige garantias reforçadas.

Em particular, o parecer alerta que as simplificações previstas na proposta — como a harmonização dos fundamentos legais, a possibilidade de tratamento de dados para fins adicionais ou a integração de novos instrumentos, como ambientes de teste regulamentares ou a utilização de inteligência artificial no âmbito do ensaio clínico — não podem reduzir os níveis de exigência do RGPD.

O CEPD e a AEPD recomenda o esclarecimento das obrigações dos responsáveis pelo tratamento de dados, a limitação dos períodos de conservação, o reforço da pseudonimização e a garantia de que qualquer acesso por parte das autoridades se limita ao estritamente necessário. Solicitam ainda que as finalidades do tratamento sejam definidas com maior precisão e que sejam integradas salvaguardas adicionais quando os dados são reutilizados para outros projetos de investigação.

## A União Europeia e o Brasil adotaram decisões mútuas de adequação que permitem a livre circulação de dados pessoais

A Comissão Europeia adotou uma decisão de adequação que reconhece que o Brasil oferece um nível de proteção de dados pessoais equivalente ao da União Europeia. Ao mesmo tempo, o Brasil adotou uma decisão recíproca. Este reconhecimento mútuo permite às empresas, entidades públicas e instituições de investigação trocar dados pessoais entre as duas jurisdições sem necessidade de salvaguardas adicionais. O objetivo é facilitar um fluxo seguro de informação e reforçar a confiança nas relações económicas e digitais entre as duas regiões.

Em conjunto, isto cria a maior zona de transferência segura de dados do mundo, beneficiando uma população combinada de aproximadamente 670 milhões de pessoas. A adoção destas decisões insere-se no contexto do Acordo de Associação entre a União Europeia e o Mercosul e do Acordo Comercial Provisório recentemente alcançado, que procura reforçar os laços económicos e políticos entre as duas regiões. A decisão europeia segue-se ao parecer do Conselho Europeu de Proteção de Dados e à validação pelos Estados-Membros através do procedimento de comitologia.

A Comissão avaliará a implementação prática da decisão de adequação num prazo de quatro anos, verificando se estão a ser mantidas as salvaguardas necessárias para a proteção dos dados pessoais.

## A Comissão Europeia designa o WhatsApp como uma plataforma online de muito grande dimensão ao abrigo do Regulamento dos Serviços Digitais

A Comissão Europeia designou oficialmente o WhatsApp como uma plataforma online de muito grande dimensão ao abrigo do Regulamento dos Serviços Digitais (DSA). Esta decisão resulta do facto de a sua funcionalidade "Canais" ter ultrapassado o limite de 45 milhões de utilizadores na União Europeia.

Embora a parte de mensagens privadas da aplicação — conversas de utilizadores, mensagens de voz, fotos e chamadas de voz e vídeo — esteja excluída do âmbito do Regulamento dos Serviços Digitais, a funcionalidade "Canais", que permite aos utilizadores divulgar informações e atualizações a um público vasto, é considerada uma plataforma online e, por conseguinte, está sujeita às obrigações deste regulamento.

Após a sua designação, a Meta — empresa proprietária do WhatsApp — tem até meados de maio de 2026 para se adaptar e cumprir as obrigações adicionais aplicáveis às plataformas de muito grande dimensão. Estas obrigações incluem a avaliação e mitigação de riscos sistémicos, como potenciais ameaças à liberdade de expressão, tentativas de manipulação eleitoral, disseminação de conteúdos ilegais e problemas de privacidade decorrentes da utilização da plataforma.

A partir desta designação, a Comissão Europeia será diretamente responsável por monitorizar a conformidade do WhatsApp com o Regulamento dos Serviços Digitais, em colaboração com o coordenador de serviços digitais da Irlanda.

## Coreia do Sul lança a primeira regulamentação abrangente de IA do mundo

Em janeiro, entrou em vigor na Coreia do Sul o primeiro conjunto abrangente de leis do mundo que regulam a inteligência artificial, visando reforçar a confiança e a segurança no setor.

Com o objetivo de se tornar uma das três principais potências mundiais em IA, a Coreia do Sul espera que a sua nova Lei de Bases sobre IA ajude a posicionar o país como líder nesta área. A legislação, na sua totalidade, entrou em vigor antes do regulamento de IA da UE, que será implementado de forma faseada até 2027.

No entanto, embora a Lei de Bases sobre IA já tenha entrado em vigor e sido implementada, o governo sul-coreano concedeu um período de carência de um ano para garantir ou facilitar a adaptação desta lei pelas empresas e pelos vários organismos públicos que devem implementá-la. Durante esta fase inicial de um ano, não serão realizadas investigações nem serão impostas quaisquer penalizações financeiras. Após o período de carência, serão aplicadas multas até 30 milhões de wones sul-coreanos.

# Decisões

## A AEPD sanciona uma empresa de energia por deficiências no seu protocolo de verificação de identidade dos clientes

A AEPD multou uma empresa de energia em um milhão de euros por violação do artigo 32.º do RGPD, relativo à segurança do tratamento de dados pessoais. A empresa não possuía medidas de segurança adequadas no seu sistema de verificação telefónica da identidade de clientes.

O processo sancionatório teve início após uma denúncia de um cliente que relatou que o endereço de correio eletrónico da sua filha tinha sido associado ao contrato de fornecimento da mesma com outra empresa do mesmo grupo, embora nenhum dos dois tivesse fornecido essa informação ou autorizado essa alteração. Embora a empresa tenha alegado ter feito a alteração de acordo com o seu protocolo de verificação de identidade, a investigação da AEPD revelou deficiências significativas no sistema.

A AEPD identificou vários problemas no protocolo de segurança da empresa. Em primeiro lugar, o sistema permitia a verificação da identidade do cliente utilizando dados que podiam ser facilmente acedidos por terceiros, como o nome completo, o número de identificação fiscal (NIF) ou o endereço postal. Em segundo lugar, não existia qualquer registo que garantisse a rastreabilidade dos dados fornecidos durante as verificações telefónicas, impossibilitando a verificação precisa das informações solicitadas em cada chamada. Em terceiro lugar, a seleção dos dados a verificar ficava ao critério de cada operador, não existindo um protocolo normalizado que garantisse um nível de segurança consistente.

Além da coima, a decisão determina que a arguida adote, no prazo máximo de três meses, medidas de segurança técnicas e organizacionais adequadas, incluindo protocolos que garantam a verificação da identidade das partes interessadas antes de qualquer alteração aos seus contratos.

## Um centro de saúde foi sancionado por apagar um CD com exames de ressonância magnética fornecidos por um paciente

O doente que apresentou a reclamação à AEPD tinha entregue ao hospital um CD com exames de ressonância magnética realizados anteriormente, destinados a servir de referência num novo exame de diagnóstico. No entanto, meses depois, quando o paciente solicitou a recuperação dos exames, o centro informou que os ficheiros tinham sido apagados.

A AEPD concluiu que estas imagens constituíam documentação clínica para todos os efeitos, independentemente de terem sido ou não integrados nos registos clínicos do doente. A Lei 41/2002, de 14 de novembro, que regula a autonomia do doente e os seus direitos e obrigações em relação à informação e documentação clínica, exige que os centros de saúde conservem este tipo de documentação durante, pelo menos, cinco anos. Ao destruir as imagens, o hospital violou este dever de custódia, o que constitui um tratamento ilícito e injustificado.

Com base no exposto, a decisão constata três infrações ao RGPD, impondo uma coima total de 1.200.000€. Em primeiro lugar, declara uma violação do artigo 9.º (categorias especiais de dados) por ter apagado dados de saúde sem nenhuma das exceções que legitimariam o seu

tratamento, o que implica uma coima de 100.000 €. Em segundo lugar, verificou-se uma violação do artigo 6.º (licitude do tratamento), uma vez que o centro não tinha fundamento legal para justificar a eliminação da documentação clínica, resultando numa outra coima de 100.000 €. Por último, considerou-se uma violação do artigo 25.º (privacidade desde a conceção e por defeito), uma vez que não existia um procedimento adequado para a gestão de suportes físicos com dados de saúde fornecidos pelos doentes, infração punida com 1.000.000 €.

A AEPD sublinha que esta não conformidade não é um incidente isolado, mas revela uma deficiência estrutural nos procedimentos do centro para gerir, armazenar e devolver a documentação clínica fornecida pelos doentes.

## A AEPD aplica uma coima de 500.000 € a um banco pela perda da documentação de um cliente

A decisão insere-se num processo sancionatório contra um banco, iniciado devido à perda de documentos apresentados por um cliente para o seu registo como novo titular de uma conta bancária. Esta perda ocorreu através de um serviço de entregas contratado pelo banco. Entre os documentos perdidos, constavam vários dados pessoais do queixoso, incluindo uma cópia integral do seu documento de identidade nacional (DNI) e do seu cônjuge. A AEPD considera provado que, após a recolha da documentação e apesar das notificações do cliente, o banco não ativou mecanismos eficazes de rastreabilidade ou de alerta precoce, limitando-se a consultas parciais e tardias, sem identificar o responsável até vários meses depois.

Assim, a AEPD constatou uma violação do artigo 32.º do RGPD, uma vez que não foram implementadas medidas técnicas e organizacionais adequadas para garantir a disponibilidade, integridade e confidencialidade dos dados, em particular no que diz respeito à rastreabilidade de envios e aos sistemas de deteção e gestão de violações, no âmbito da responsabilidade proativa dos artigos 5.º, n.º 2 e 24.º do RGPD. Da mesma forma, a AEPD refere o artigo 28.º do RGPD relativo à seleção e controlo do responsável pelo tratamento de dados, embora tal não constitua uma infração autónoma.

A AEPD destaca a negligência da entidade demandada na monitorização do incidente e considera a sensibilidade de alguns dos dados afetados (cartão de cidadão e informação bancária), aplicando uma coima de 500.000 €. O processo concluiu-se com o pagamento voluntário por parte da entidade demandada, reduzindo a coima para 400.000 €, e a decisão tornou-se definitiva.

## A CNIL sanciona com 42 milhões de euros um grupo de telecomunicações por uma falha de segurança

A autoridade francesa de proteção de dados (CNIL) aplicou duas coimas, no total de 42 milhões de euros, a duas empresas pertencentes ao mesmo grupo de telecomunicações, após uma violação de segurança que permitiu a um atacante aceder a informação de mais de 24 milhões de contratos de assinantes. Os dados comprometidos incluíam identificadores bancários, que são particularmente sensíveis devido à sua natureza pessoal e aos riscos associados à utilização fraudulenta.

A análise da autoridade revelou várias violações do RGPD. Em primeiro lugar, foi constatada uma violação do artigo 32.º do RGPD, uma vez que não tinham sido implementadas medidas básicas de segurança que teriam impedido o acesso não autorizado. A autenticação para o acesso a sistemas internos, incluindo o acesso remoto dos colaboradores através de VPN, não era suficientemente robusta, e os mecanismos para a deteção de comportamentos anómalos revelaram-se ineficazes.

Em segundo lugar, foi constatada uma violação do artigo 34.º do RGPD relativamente à comunicação enviada aos afetados pela violação. A mensagem inicial enviada não incluía toda a informação necessária para compreender a dimensão do incidente nem as medidas de autoproteção recomendadas, dificultando a resposta imediata dos utilizadores.

Por fim, no caso de uma das entidades responsáveis pelos serviços de telemóvel, foi também constatada uma violação do artigo 5.º, n.º 1, alínea e) do RGPD por reter dados de ex-subscritores durante anos sem justificação,

indo para além do tempo necessário para cumprir as correspondentes obrigações contabilísticas.

## Sancionado um fornecedor de energia por cruzamento de dados pessoais de dois clientes

A violação ocorreu quando um cliente do fornecedor de energia recebeu um e-mail com dados pessoais de terceiros, incluindo o seu nome completo, número de contrato, faturas e a existência de uma dívida pendente. A receção do referido e-mail pelo reclamante ocorreu porque um funcionário do subcontratante para o tratamento de dados da empresa fornecedora atribuiu erradamente o endereço de e-mail do reclamante a um cliente terceiro.

O erro ocorreu porque o funcionário estava a atender dois utilizadores em simultâneo por chat, o que levou à inserção inadvertida do endereço de e-mail do reclamante no registo de outro cliente. Este canal de chat, que registou mais de 15.000 interações em 2023, permitia a um agente gerir várias conversas em simultâneo, aumentando significativamente o risco de erros. Apesar de a empresa ter removido o canal de chat em 2024, a AEPD considera esta ação reativa, e não preventiva.

Enquanto a proposta inicial previa uma coima de 1.000.000 €, a decisão fixa uma coima de 500.000 € por violação do artigo 25.º do RGPD, relativo à proteção de dados desde a conceção e por defeito.

Como fundamento para a sua decisão, a Agência conclui que a empresa não dispunha de medidas técnicas e organizacionais adequadas para prevenir imprecisões nos dados, tais como controlos eficazes para detetar duplicados ou atribuições incorretas entre clientes. Os mecanismos existentes apenas verificavam aspetos formais, mas não impediam que os mesmos dados fossem atribuídos a duas pessoas diferentes. Esta falta de controlos e de uma análise de risco adequada demonstra, segundo a Agência Espanhola de Proteção de Dados (AEPD), uma falha sistémica na conceção do processo de atualização de dados, que potencialmente expôs todos os clientes da entidade a incidentes semelhantes.

## A AEPD impõe uma sanção a uma empresa de telemóveis por roubo de identidade do titular de uma linha telefónica

A decisão analisa uma reclamação contra uma empresa de telemóveis pela perda do serviço telefónico e por transações bancárias fraudulentas sofridas pelo reclamante após uma alteração não autorizada da titularidade da linha e a criação de um cartão SIM duplicado.

Neste caso, a alteração de titularidade foi tratada telefonicamente sem seguir o protocolo interno da empresa. O processo de verificação reforçada, que envolve uma chamada de verificação para a linha ou o envio de um OTP (*one-time password*), e a verificação dos últimos dígitos da fatura, foram omitidos. A chamada não teve origem na linha afetada. Em relação à substituição do cartão SIM, a verificação através de um código temporário ou chamada também não foi realizada, sendo que o documento de identidade digitalizado pertencia a um terceiro que não o reclamante.

Assim, a AEPD considera que a identificação do verdadeiro titular e a licitude do tratamento não foram garantidas, permitindo, assim, o tratamento sem uma base jurídica válida, em violação do artigo 6.º, n.º 1 do RGPD. A responsabilidade baseia-se na falta de diligência na verificação da identidade, na falha no cumprimento da responsabilidade proativa (artigos 5.º, n.º 2 e 24.º do RGPD) e na doutrina do Supremo Tribunal sobre o roubo de identidade, que fundamenta a responsabilidade na ausência de controlos para garantir uma base jurídica suficiente para o tratamento.

Por último, a AEPD considera as duas operações de tratamento ilícito relacionadas (alteração de titularidade e duplicação de cartão SIM) como uma única infração ao artigo 6.º, n.º 1 do RGPD, impondo uma coima de 300.000 €.

## A AEPD reitera que os telemóveis pessoais dos colaboradores não podem ser utilizados como ferramenta de autenticação no local de trabalho

A AEPD voltou a declarar ilícita a comunicação dos números de telefone pessoais dos colaboradores por uma empresa de *contact center* a um dos seus clientes internacionais para ativar um sistema de autenticação de dois fatores necessário para aceder às suas ferramentas empresariais. A prática afetou mais de 200 colaboradores e durou mais de um ano.

A empresa implementou um sistema de acesso às ferramentas de um cliente internacional que obrigava à receção de códigos de autenticação nos telemóveis dos colaboradores. Durante a formação inicial, foi pedido aos colaboradores que escrevessem o seu número de telefone pessoal e a data de nascimento numa folha de papel. Posteriormente, começaram a receber os códigos de acesso diretamente do cliente. Os representantes sindicais propuseram alternativas, como o uso do e-mail empresarial, mas a empresa respondeu que isso não era viável porque o cliente exigia a vinculação de um número de telefone para gerar um token de autenticação de dois fatores, e a empresa não dispunha de terminais profissionais suficientes. A própria empresa reconheceu que estava em transição gradual para telefones e cartões SIM empresariais, indicando que 203 dos seus 364 funcionários ainda utilizavam os seus números pessoais.

A Agência está a analisar o caso à luz do artigo 6.º, n.º 1, alínea b) do RGPD, que permite o tratamento de dados pessoais apenas quando estritamente necessário para a execução do contrato com o trabalhador. De acordo com a Agência Espanhola de Proteção de Dados (AEPD), este requisito não foi cumprido, uma vez que cabe ao empregador fornecer o equipamento necessário para a execução do trabalho, em conformidade com o princípio dos recursos fornecidos pelo empregador inerentes à relação laboral. Por isso, e considerando que existiam opções menos intrusivas (e-mail empresarial ou terminais profissionais), o telefone pessoal não pode ser considerado essencial para a prestação do serviço.

A decisão sublinha ainda que a empresa tinha plena consciência da irregularidade: o seu encarregado da proteção de dados tinha alertado por escrito que a utilização de telemóveis pessoais para fins profissionais violava a legislação. Apesar disso, a organização continuou a enviar dados ao cliente sem fornecer alternativas técnicas ou adotar medidas de minimização adequadas.

Por estas razões, a autoridade constatou uma infração ao artigo 6.º do RGPD e aplicou uma coima de 80.000 €, posteriormente reduzida para 48.000 € devido ao reconhecimento de responsabilidade e ao pagamento voluntário. Como nota adicional, a decisão apresenta alguma inconsistência na análise do papel da empresa, classificando-a inicialmente como subcontratante para o tratamento e, posteriormente, como responsável pelo tratamento.

## Possível alteração de critério da AEPD em relação à utilização de tecnologias biométricas

A AEPD arquiva um processo relativo à utilização de dados biométricos no controlo de acessos a determinadas áreas de produção por uma empresa do setor alimentar.

Esta decisão é de particular interesse, dado que a AEPD encerrou o caso sem constatar qualquer infração relacionada com a utilização de tecnologias de identificação biométrica. Isto representa uma possível mudança na postura da AEPD, que anteriormente adotava uma abordagem restritiva à utilização destas tecnologias para o controlo de acessos no local de trabalho.

Neste caso, segundo a decisão, a empresa justificou a necessidade do controlo com base em requisitos sanitários, avaliou alternativas e restringiu a sua implementação à área de produção, em vez de a adotar de forma geral e indiscriminada. O controlo biométrico aplicava-se apenas a uma área de acesso restrito por motivos sanitários relacionados com o setor alimentar, o que poderia justificar a necessidade da medida.

Contudo, a AEPD não inclui na decisão uma análise detalhada dos fundamentos legais aplicáveis ou das possíveis autorizações para o tratamento dessas informações, nos termos do

Artigo 9.º, n.º 2 do RGPD, esta decisão indica uma possível mudança de abordagem na utilização destas tecnologias e define algumas orientações relativas aos requisitos que devem ser cumpridos para implementar este tipo de tecnologia no local de trabalho.

## Coima por extravio de atestados médicos em local público

A AEPD sancionou uma empresa especializada em serviços de prevenção de riscos profissionais em 100.000 euros pela exposição acidental de atestados médicos pertencentes a agentes de diversas forças policiais. A documentação, que continha dados de saúde particularmente sensíveis, foi encontrada abandonada em local público após ter sido transportada das instalações oficiais para as instalações da empresa.

A investigação revelou deficiências significativas nos procedimentos internos: ausência de cadeia de custódia, falta de registos relativos à transferência da documentação e ausência de medidas organizacionais para garantir a sua confidencialidade. A autoridade conclui que estas ações constituem uma violação do princípio da integridade e confidencialidade previsto no artigo 5.º, n.º 1, alínea f) do RGPD, justificando, assim, a aplicação da coima.

Além da coima, a decisão determina que a entidade implemente medidas que garantam a rastreabilidade e a proteção da documentação médica quando manuseada fora das suas instalações. A AEPD reitera que o tratamento de dados de saúde exige uma maior diligência e que os responsáveis por este tipo de serviços devem garantir medidas de segurança proporcionais ao risco decorrente da sua atividade.

## Um hotel é sancionado por divulgação indevida de dados pessoais de clientes

Nesta decisão, a AEPD analisa uma reclamação apresentada através do sistema IMI (Sistema de Informação do Mercado Interno) pela Autoridade Sueca de Proteção de Dados contra uma empresa hoteleira relativamente à divulgação indevida de dados pessoais de proprietários e hóspedes de um complexo turístico.

O pessoal de segurança, atuando como responsáveis pelo tratamento de dados contratados pela empresa, deixaram listas em papel com dados como o nome, apelido, país, número do apartamento, passaporte e números de documentos de identidade à vista de terceiros, que chegaram mesmo a fotografá-las. A AEPD constatou que, apesar de a empresa possuir protocolos genéricos e, posteriormente, ter fornecido documentação sobre auditorias, protocolos internos e medidas adotadas, não foi demonstrada a existência de medidas técnicas e organizacionais adequadas para impedir o acesso não autorizado aos dados. Por conseguinte, a AEPD concluiu que ocorreu uma violação da confidencialidade e que as medidas alegadas não eram suficientes nem especificadas para garantir a segurança exigida pelo RGPD.

Foi aplicada uma coima de 40.000 €, tendo em conta a natureza e gravidade da infração, o volume de dados expostos, a sensibilidade da informação (cartão de cidadão e passaporte) e a relação da atividade do responsável com o tratamento contínuo dos dados pessoais. A empresa sancionada optou pelo pagamento voluntário, aplicando-se uma redução de 20%, o que reduz a coima final para 32.000€. Além disso, a empresa foi intimada a demonstrar, no prazo de três meses, a implementação de medidas adequadas para prevenir futuros incidentes deste tipo.

## Uma clínica dentária foi sancionada por gravar imagens e sons dentro do consultório

A decisão analisa um caso em que um ex-funcionário de uma clínica dentária relatou a gravação de imagens e sons por câmaras de vigilância sem informação adequada, alegando que não existia sinalização informativa e que os pacientes não eram avisados da gravação durante os procedimentos. A clínica alegou que possuía dois dispositivos: uma câmara de vídeo no consultório dentário e uma câmara fotográfica na receção, ambas para fins de segurança e geridas por uma empresa externa. A clínica reconheceu que o sistema gravava o som na sala de tratamento e que as imagens eram armazenadas por um período máximo de sete dias.

A AEPD considerou que a gravação contínua de pacientes durante os tratamentos dentários

era desproporcional aos objetivos de segurança invocados, violando o princípio de minimização de dados (Art. 5.º, n.º 1, alínea c) do RGPD). A Agência sublinhou que a gravação de conversas entre doentes e funcionários constitui uma intrusão ilícita no direito à privacidade, ordenando a reorientação ou remoção da câmara no prazo de três meses.

Para efeitos sancionatórios, foi aplicada uma coima de 2.000 €, nos termos do artigo 83.º, n.º 5 do RGPD (princípios básicos e condições de licitude), tendo em conta a natureza das ações, o seu alcance e o impacto nos direitos fundamentais. Durante o processo, a clínica assumiu a responsabilidade e fez um pagamento voluntário, reduzindo assim a coima para 1.200 €. A AEPD declarou a prática da infração, confirmou a coima resultante e decidiu encerrar o processo.

## Um sindicato da área da saúde e a sua fundação foram sancionados por uma violação de segurança e falta de transparência na sua corresponsabilidade

A autoridade de controlo sancionou um sindicato da área da saúde e a sua fundação, ligada à formação em enfermagem, em 15.000 euros após ter constatado duas violações graves no âmbito de um ataque de *ransomware* que comprometeu os dados de quase 198.000 pessoas. Ambas as entidades atuavam como corresponsáveis pelo tratamento no desenvolvimento do seu programa de formação conjunto para profissionais de saúde.

O incidente ocorreu quando um grupo identificado como *Hunters International* acedeu aos seus sistemas, encriptou a informação e ofereceu publicamente as bases de dados para venda na *dark web*. Embora a notificação enviada à autoridade indicasse que apenas os dados geridos para fins de formação foram afetados, a investigação sugere que outras áreas podem ter sido comprometidas. A autoridade refere que não há registo de notificação às partes potencialmente afetadas fora do ambiente de formação, o que levanta dúvidas sobre a exatidão da avaliação do verdadeiro alcance da violação.

A decisão constata uma violação do artigo 5.º, n.º 1, alínea f) do RGPD, uma vez que foi determinado que, antes do ataque, não existia uma análise de risco suficiente nem medidas técnicas e organizacionais adequadas em vigor. Entre as deficiências identificadas estão a ausência de autenticação multifatorial, bases de dados não encriptadas e capacidade insuficiente para detetar e avaliar adequadamente o incidente, bem como a falta de monitorização do seu impacto e duração.

Além disso, a autoridade considera que ocorreu violação do artigo 26.º do RGPD, referindo que ambas as entidades se declararam corresponsáveis pelos dados através de um acordo genérico, sem especificar de forma transparente as respetivas responsabilidades. Este acordo também não foi disponibilizado aos participantes nas atividades de formação, e as informações fornecidas nos formulários e políticas de privacidade não refletiam a real corresponsabilidade entre as duas organizações.

## A AEPD sanciona uma operadora de telecomunicações por enviar credenciais de acesso à área de cliente num e-mail em texto simples

A AEPD proferiu uma decisão que impõe uma multa de 10.000 euros a um operador de telecomunicações por violação do artigo 32.º do RGPD. O processo teve início após uma reclamação de um cliente que recebeu um e-mail, enviado em texto simples e não encriptado, em que a empresa o notificava sobre uma atualização da sua área de cliente, incluindo as suas credenciais de acesso completas (nome de utilizador e palavra-passe). O reclamante relatou que o referido portal, que armazena dados como o nome, apelido, morada, número do documento de identidade, número de telefone, dados bancários, faturas e registos de utilização, também não possuía autenticação de dois fatores.

A entidade sancionada argumentou que o incidente foi o resultado de um único erro humano, que atuou imediatamente redefinindo as palavras-passe e contactando a parte afetada, e que não houve acesso não autorizado nem exfiltração de dados. No entanto, a AEPD rejeita estes argumentos,

salientando que o artigo 32.º do RGPD impõe uma obrigação de meios que exige uma avaliação de risco eficaz, e que o envio de credenciais em texto simples por e-mail demonstra a falta de medidas organizacionais suficientes para evitar a divulgação indevida de informações de autenticação. A Agência sublinha que não é necessário que ocorra um dano efetivo para que haja uma infração; basta que as medidas de segurança sejam inadequadas ao risco inerente ao tratamento.

Como circunstâncias atenuantes, a AEPD considerou a resposta rápida da empresa e a adoção de medidas corretivas. Como fatores agravantes, citou a negligência grave no cumprimento das normas e a ligação da sua atividade ao tratamento em massa de dados pessoais de clientes.

## A AEPD sanciona uma instituição de crédito online por exigir aos seus clientes uma fotografia sua a segurar o cartão de cidadão para processar o cancelamento de um empréstimo

A AEPD proferiu uma decisão que sanciona uma instituição de crédito online por violação do artigo 5.º, n.º 1, alínea c) do RGPD, relativo ao princípio da minimização de dados. O procedimento teve início após uma reclamação de um cliente que, tendo solicitado o cancelamento antecipado do seu empréstimo, foi obrigado, como condição para o processamento, a fornecer uma fotografia em que aparecia a segurar o seu documento de identidade.

A entidade argumentou que este procedimento de identificação estava em conformidade com as obrigações estabelecidas na legislação de combate ao branqueamento de capitais. A AEPD rejeitou esta justificação, afirmando que as normas setoriais invocadas não são contrárias nem incompatíveis com os princípios do RGPD e que ambos os quadros regulamentares devem ser aplicados concomitantemente. Em particular, a Agência sublinha que a Lei 10/2010, de 28 de abril, relativa à prevenção do branqueamento de capitais, estabelece uma obrigação de identificação que pode ser cumprida por outros meios menos intrusivos, como uma assinatura eletrónica qualificada, uma cópia do documento de identidade emitida por um notário público ou a verificação através dos sistemas de identificação já disponibilizados pela entidade aos seus clientes. Solicitar uma fotografia ao interessado com o seu documento de identidade nacional constitui um tratamento excessivo de dados pessoais, gerando riscos adicionais de roubo de identidade.

A coima inicialmente proposta era de 10.000 €, mas a entidade optou pelo pagamento voluntário com uma redução de 20%, reduzindo a coima para 8.000 €. Além disso, a AEPD ordenou à entidade que adote medidas para garantir que a verificação de identidade nos procedimentos de cancelamento de empréstimos é realizada, daqui para a frente, utilizando opções que garantam o cumprimento do princípio da minimização de dados.

## A AEPD acolhe uma reclamação contra o Serviço de Saúde das Ilhas Baleares por não ter cumprido o direito de acesso de um cidadão

A AEPD resolveu o procedimento de direitos iniciado na sequência de uma reclamação de um cidadão que exerceu o seu direito de acesso à informação junto do Serviço de Saúde das Ilhas Baleares (IBSALUT), sem ter recebido a resposta legalmente exigida ao seu pedido.

A decisão da AEPD reitera que, em conformidade com o artigo 12.º do RGPD e a Lei Espanhola de Proteção de Dados (LOPD-gdd), o responsável pelo tratamento de dados deve estabelecer procedimentos e mecanismos para facilitar o exercício dos direitos do titular dos dados e é obrigado a responder aos pedidos no prazo de um mês, indicando os motivos do incumprimento. O ónus da prova quanto ao cumprimento da obrigação de responder ao pedido do titular dos dados para exercer os seus direitos recai sobre o responsável pelo tratamento dos dados, devendo a comunicação enviada ao titular dos dados ser concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples.

A AEPD salienta que a legislação aplicável não permite que o pedido seja ignorado como se não tivesse sido submetido, ficando sem a resposta a que os responsáveis pelo

tratamento de dados são obrigados, mesmo que não existam dados relativos ao titular dos dados a tratar ou mesmo nos casos em que o pedido não cumpra os requisitos estabelecidos. Neste caso, o destinatário é também obrigado a solicitar a correção das deficiências verificadas ou, se for caso disso, a negar o pedido com uma justificação fundamentada, indicando as razões pelas quais o direito em causa não pode ser atendido.

Consequentemente, a AEPD deferiu a reclamação, considerando que houve violação do disposto no artigo 15.º do RGPD, e insta o Serviço de Saúde das Ilhas Baleares a enviar ao reclamante, no prazo de dez dias úteis a contar da data em que a decisão se torne definitiva e executória, um certificado que conceda o direito de acesso exercido ou que o negue com uma justificação fundamentada, indicando as razões pelas quais o pedido não pode ser atendido.

## A AEPD sancionou uma empresa de entregas por subcontratação não autorizada na cadeia de tratamento de dados

A AEPD sancionou uma empresa de logística por várias irregularidades na gestão da subcontratação dentro da cadeia de processamento de dados. O problema surgiu quando um cliente descobriu que, para processar uma remessa, os seus dados tinham sido partilhados com terceiros não incluídos na lista autorizada de subcontratantes para o tratamento de dados.

Após análise da documentação fornecida pelas empresas envolvidas, a AEPD concluiu que ocorreram três violações distintas do RGPD. Em primeiro lugar, a subcontratante para o tratamento de dados realizou uma subcontratação não autorizada a outra empresa de logística, violando o artigo 28.º, n.º 2, que exige o consentimento prévio e específico do responsável pelo tratamento de dados. Em segundo lugar, não informou adequadamente o responsável pelo tratamento de dados de que este subcontratante, por sua vez, tinha contratado um terceiro, o que reforça a violação da mesma disposição. Por último, a AEPD adverte que não existia um contrato de subcontratação válido entre a demandada e o primeiro subcontratante, violando assim o artigo 28.º, n.º 4, que exige a documentação das obrigações aplicáveis ao tratamento.

Cada uma destas infrações implica uma coima independente de 5.000 €, totalizando 15.000 €.

## Uma entidade de saúde enviou por erro os dados pessoais dos doentes de reprodução assistida para outros utentes do serviço

Em abril de 2023, a AEPD recebeu uma denúncia de uma pessoa que relatou que a unidade de reprodução assistida do centro onde tinha sido paciente tinha enviado um e-mail a anunciar a transferência do serviço para uma nova entidade, contendo os dados pessoais de outros pacientes.

A entidade em causa utilizava um sistema automatizado com documentos combinados em Word e Excel contendo dados pessoais dos pacientes (nome, apelido, número do documento de identidade nacional e endereço de e-mail), gerando PDF que eram enviados automaticamente por e-mail. O processo funcionou corretamente nos primeiros 299 envios, mas a partir do documento 300, começou a enviar informação para destinatários incorretos. Assim sendo, pelo menos 237 doentes receberam os dados pessoais de outros utilizadores (nome, apelido, número do documento de identidade nacional e estado de doente de reprodução assistida), de um total de 637 indivíduos potencialmente afetados. A violação foi comunicada à AEPD e às partes afetadas.

A AEPD identificou duas infrações ao RGPD neste processo sancionatório: (i) a violação do princípio da integridade e confidencialidade (Art. 5.º, n.º 1, alínea f) por não encriptar as notificações, apesar de ser internamente obrigada a fazê-lo, e (ii) incumprimento do Artigo 35.º por não ter realizado uma avaliação de impacto sobre a proteção de dados (AIPD) para o tratamento em larga escala de dados de saúde. A AEPD rejeitou os argumentos da empresa reclamada relativamente à pré-existência do RGPD e à sua adaptação através de uma análise de risco, e enfatizou a auditoria de 2020, que já alertava para a necessidade de realizar uma AIPD.

A AEPD propôs uma coima total de 100.000 euros (50.000 por infração). Após o pagamento

voluntário com uma redução de 20%, a coima final foi de 80.000 €.

## Imposição de coima por tratamento de dados biométricos sem fundamento jurídico válido e retenção excessiva de dados pessoais

A AEPD aplicou uma coima de 950.000 euros a uma empresa especializada na verificação de identidade e idade em ambientes digitais por tratar dados biométricos sem fundamento jurídico legítimo, nos termos do Artigo 9.º, n.º 2 do RGPD, obter consentimento inválido e reter dados por tempo superior ao necessário.

Ao registar-se no serviço, o utilizador realiza um processo de verificação em que a sua imagem facial é captada. A partir desta captura, é gerado e armazenado um modelo biométrico, sendo utilizado para autenticar o utilizador e confirmar a sua identidade em acessos ou interações subsequentes. A AEPD conclui que este processo envolve a identificação inequívoca de uma pessoa singular, constituindo o tratamento de categorias especiais de dados, nos termos do artigo 9.º, n.º 1 do RGPD. A empresa alegou que o seu sistema não "identificava" o utilizador. No entanto, ao não reconhecer a natureza especial dos dados tratados, não aplicou nenhuma das bases legais do artigo 9.º, n.º 2 do RGPD e, por conseguinte, o consentimento obtido foi considerado inválido.

Além disso, a obtenção de consentimento para fins de investigação e melhoria através de uma quadrícula pré-selecionada é penalizada, uma vez que é incompatível com o consentimento livre, específico, informado e inequívoco (artigo 7.º do RGPD). Por último, verificou-se uma violação do princípio da limitação da conservação, uma vez que os dados pessoais foram conservados por um período superior ao estritamente necessário, sem critérios eficazes para o seu apagamento (artigo 5.º, n.º 1, alínea e) do RGPD).

## A AEPD sancionou uma empresa pelo tratamento indevido de dados pessoais por um dos seus representantes de vendas

A AEPD proferiu uma decisão que aplica uma coima de 20.000 euros e outra de 200.000 euros por violação dos artigos 13.º e 6.º do RGPD, respetivamente, a uma empresa do setor energético.

A controvérsia surgiu de uma chamada telefónica feita a um cliente por um representante de vendas da empresa, seguida de um e-mail para o mesmo cliente contendo dados pessoais previamente preenchidos. Tal como em inúmeros casos semelhantes, o reclamante alega não ter tido qualquer contacto ou relacionamento prévio com a empresa, cujos produtos e serviços estavam a ser promovidos pelo comercial.

A demandada argumentou que, no momento do envio das comunicações, o vendedor atuava como responsável pelo tratamento de dados independente e que, por isso, qualquer tratamento de dados indevido por parte deste deveria acarretar responsabilidade para o vendedor e não para a demandada. No entanto, a AEPD realizou uma análise detalhada dos conceitos de responsável pelo tratamento e operador de dados, concluindo que, atentas as especificidades do caso, a demandada determinou as finalidades e os meios do tratamento e, por isso, era de facto o responsável pelo tratamento dos dados. Consequentemente, a AEPD constatou uma violação do dever de informação e da existência de uma base legal suficiente para o envio de tais comunicações, uma vez que a demandada não tinha qualquer relação com a reclamante.

Esta decisão fornece informações importantes a considerar na determinação das funções e serve de alerta contra práticas generalizadas em determinados setores, em que as informações dos titulares dos dados são partilhadas de forma demasiado livre entre empresas comerciais e prestadores de diversos serviços.

## Sanção decorrente de um incidente de segurança

Nesta decisão, a AEPD constata uma violação dos artigos 5.º, n.º 1, alínea f), 32.º, 33.º e 34.º do RGPD na sequência de um incidente de segurança sofrido pela demandada, que afetou até um milhão de registos, e impõe uma coima total de € 1.090.000.

Embora existam várias decisões semelhantes que, como neste caso, debatem o nível de diligência da entidade na implementação de medidas de segurança e gestão de incidentes, esta resolução é particularmente interessante por conter referências a questões que, embora já bem conhecidas, não são menos relevantes e interessantes. Destacamos as seguintes:

- O prazo de 72 horas para notificar a AEPD sobre um incidente de segurança deve ser calculado em dias de calendário, e o facto de o prazo coincidir com um feriado não constitui motivo válido para o atraso na notificação.
- A AEPD está a aplicar uma sanção conjunta por infração dos artigos 5.º, n.º 1, alínea f) e 32.º do RGPD, tal como já tem feito repetidamente. Embora seja verdade que recentemente foram emitidas algumas decisões que se limitam a um dos dois artigos e não a ambos, a AEPD está a retomar esta abordagem, argumentando que a sanção "dupla" não constitui uma violação do princípio non bis in idem, e que as duas sanções são perfeitamente compatíveis.

Esta matéria é tema de debate recorrente nas decisões da AEPD e também nos tribunais, pelo que será importante acompanhá-la de perto para se manter informado sobre os seus desenvolvimentos.

# Acórdãos

## O Tribunal de Justiça da União Europeia (TJUE) pronuncia-se sobre a legislação nacional relativa ao tratamento de dados biométricos

Neste acórdão, o TJUE respondeu a diversas questões prejudiciais relativas à aplicação da legislação nacional francesa que transpõe a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou à execução de sanções penais, e à livre circulação desses dados.

O caso teve origem em França, onde uma pessoa foi detida durante uma manifestação e recusou submeter-se à recolha de impressões digitais e a ser fotografada. Embora tenha sido absolvida da principal infração em causa, foi multada em 300 euros por se ter recusado a prestar informações de identificação, nos termos do artigo 55.º, n.º 1 do Código de Processo Penal francês. Na sequência de recursos simultâneos, os tribunais franceses submeteram três questões prejudiciais ao Tribunal de Justiça da União Europeia (TJUE) para determinar a compatibilidade desta legislação com a Diretiva (UE) 2016/680.

A discussão centra-se sobretudo na medida em que a legislação nacional pode exigir a recolha de dados particularmente sensíveis, como os dados biométricos. A este propósito, o TJUE conclui que:

- A legislação nacional que estabelece a recolha sistemática de dados biométricos de qualquer pessoa suspeita de ter cometido ou tentado cometer um crime é contrária ao direito da UE, a menos que se verifiquem duas condições: (i) que a legislação nacional defina de forma adequada e suficiente as finalidades específicas e concretas dessa recolha, e (ii) que a autoridade competente seja obrigada a avaliar, caso a caso, se a recolha é estritamente necessária para atingir essas finalidades, de modo a que a recolha não seja sistemática.

- A autoridade competente deve justificar adequadamente, em cada caso concreto, por que razão a recolha de dados biométricos é "estritamente necessária". O Tribunal esclarece que esta justificação pode ser concisa, mas deve ser suficientemente clara para que a parte afetada compreenda as razões da medida e possa exercer o seu direito a um recurso efetivo.

- Quanto à legalidade da sanção por falta de cooperação com as autoridades, o TJUE conclui que o direito da UE não impede um Estado-Membro de impor sanções penais por recusa em submeter-se à recolha de dados biométricos. Contudo, esta sanção só será legal se a recolha de dados cumprir o requisito de ser "estritamente necessária" e se a sanção imposta respeitar o princípio da proporcionalidade.

Esta decisão é de particular interesse no contexto das atividades das forças de segurança do Estado, uma vez que fornece orientações importantes sobre as suas competências e os requisitos que devem ser cumpridos na legislação nacional para autorizar estes organismos a recolher determinados tipos de dados.

## O recurso interposto pelo WhatsApp Ireland contra a decisão vinculativa do Conselho Europeu de Proteção de Dados é admissível

A questão em apreço nesta decisão remonta a um processo iniciado em dezembro de 2018 pela Autoridade de Proteção de Dados da Irlanda (*Data Protection Commission* ou DPC), enquanto autoridade de controlo principal, contra a WhatsApp Ireland Ltd (WhatsApp) por uma alegada violação das obrigações de transparência e informação previstas nos artigos 12.º a 14.º do RGPD. Após uma proposta inicial de resolução emitida pela DPC e submetida às outras autoridades nacionais de controlo envolvidas, oito delas apresentaram contestações pertinentes e fundamentadas, o que levou ao encaminhamento do litígio para o Comité Europeu de Proteção de Dados (CEPD), nos termos do artigo 65.º, n.º 1, alínea a), do RGPD.

A este respeito, em julho de 2021, o CEPD adotou a Decisão Vinculativa 1/2021, que considerou ter ocorrido uma infração às disposições supracitadas do RGPD, obrigando a DPC a modificar as medidas corretivas planeadas e, em particular, o valor das coimas. Com base no exposto, a DPC adotou uma decisão final em que, entre outras medidas, aplicou uma série de coimas ao WhatsApp, no total de 225 milhões de euros.

Em resposta a esta decisão, o WhatsApp interpôs recurso de anulação da decisão vinculativa do CEPD junto do Tribunal Geral. No entanto, o Tribunal Geral declarou o recurso inadmissível, uma vez que a decisão não era um ato passível de impugnação e não afetava diretamente o WhatsApp. A este respeito, o Tribunal Geral observou que a decisão era uma medida provisória (e não definitiva) e que apenas a decisão final poderia ser impugnada perante um tribunal nacional. O WhatsApp recorreu desta decisão para o TJUE, questão que é resolvida por este acórdão.

Portanto, as questões jurídicas resolvidas no acórdão são essencialmente duas: (i) a natureza impugnada da decisão vinculativa do CEPD e (ii) o requisito de impacto direto no requerente.

Em primeiro lugar, no que respeita à natureza impugnável do ato, nos termos do artigo 263.º do Tratado sobre o Funcionamento da União Europeia (TFUE), o TJUE recorda que uma ação de anulação pode ser intentada contra todos os atos adotados por instituições, órgãos, gabinetes ou entidades da União que tenham por objetivo produzir efeitos juridicamente vinculativos. Deve ser considerada a essência do ato e os seus efeitos examinados à luz de critérios objetivos, como o seu conteúdo, o contexto da sua adoção e as competências do órgão autor do ato, entre outros. A este propósito, o TJUE rejeita expressamente a qualificação do ato como uma "medida provisória" feita pelo Tribunal Geral, esclarecendo que a decisão do CEPD estabelece definitivamente a posição daquele órgão sobre as questões que lhe competem resolver, esgotando assim a sua esfera de competência.

Por outro lado, no que respeita ao requisito do impacto direto previsto no n.º 4 do artigo 263.º do TFUE, o Tribunal aplica a sua jurisprudência consolidada, que exige o cumprimento de duas condições cumulativas: que o ato afete diretamente a situação jurídica do requerente e que não deixe margem para discricionariedade por parte dos destinatários responsáveis pela sua aplicação. Consequentemente, o TJUE conclui que a decisão do CEPD modifica substancialmente a situação jurídica do WhatsApp ao declarar infrações adicionais ao RGPD — especificamente aos artigos 13.º, n.º 1, alínea d), e 13.º, n.º 2, alínea e), que obrigam a empresa a modificar a sua relação contratual com os utilizadores do serviço de mensagens prestado. Conclui-se, assim, que existe uma ligação direta entre a decisão e os seus efeitos na situação do WhatsApp.

Com base no exposto, o Tribunal de Justiça da União Europeia (TJUE) declarou admissível o recurso do WhatsApp, anulando a decisão do Tribunal Geral e remetendo o caso de volta para o Tribunal Geral para que este se pronuncie sobre o mérito, incluindo a questão de saber se o WhatsApp infringiu as obrigações de transparência e informação estabelecidas nos artigos 12.º a 14.º do RGPD.

## Anuladas várias sanções impostas pela AEPD a uma seguradora pelo envio de comunicações comerciais para endereços de correio eletrónico genéricos

O Primeiro Juízo da Secção de Contencioso-Administrativo da Audiência Nacional aceitou o recurso interposto por uma conhecida seguradora contra a deliberação emitida pela AEPD em abril de 2022, que confirmou a aplicação de três coimas de 100.000 euros cada, por infrações aos artigos 6.º, 28.º e 17.º do RGPD.

O procedimento sancionatório teve origem numa reclamação apresentada por uma pessoa que, entre 2016 e 2020, solicitou repetidamente a eliminação dos seus dados pessoais sem obter resposta, continuando a receber comunicações publicitárias num endereço de email genérico (info@.....), registado na Lista Robinson.

A Secção fundamentou a sua decisão de acolher o recurso em vários motivos. Em primeiro lugar, concluiu que um endereço de correio eletrónico genérico como info@empresa.com não constitui dados pessoais para efeitos do artigo 4.º do RGPD, uma vez que não permite a identificação direta ou indireta de uma determinada pessoa singular. Em segundo lugar, determinou que o responsável pelo tratamento dos dados não era a própria seguradora, mas sim os agentes de seguros que, independentemente, recolhiam e geriam os dados como responsáveis distintos, sem qualquer indício de uma base de dados partilhada. Por último, o Tribunal constata que, assim que a reclamação do requerente foi comunicada, este foi informado da inexistência de dados nos sistemas da seguradora e o seu nome foi removido das listas dos agentes.

Consequentemente, a Audiência Nacional anula as três sanções impostas, com a imputação expressa de custas à Administração demandada.

## A Audiência Nacional confirma a improcedência de uma reclamação pela perda de um relatório médico, considerando os factos prescritos

Após a apresentação de uma reclamação junto da AEPD relativa à perda de um relatório médico de 2015 referente ao pai da reclamante, que, segundo a mesma, evidenciava uma violação de segurança, a AEPD indeferiu a reclamação por dois motivos: a prescrição e a inaplicabilidade da legislação de proteção de dados a pessoas falecidas, exceto nos casos previstos no artigo 3.º da Lei Espanhola de Proteção de Dados (LOPD-gdd).

Em sede de recurso, a Audiência Nacional confirma o indeferimento da AEPD, embora atenue alguns aspetos. Em primeiro lugar, concorda que os factos estavam realmente prescritos. Contudo, rejeita o argumento relativo ao enquadramento jurídico aplicável a pessoas falecidas, uma vez que o paciente ainda estava vivo quando o relatório desaparecido foi elaborado. Em segundo lugar, o Tribunal esclarece que o ocorrido não constitui uma violação da segurança do sistema, mas antes um problema de gestão e registo de documentos: o médico considerou o documento um rascunho e, por isso, não o incluiu no registo médico.

A decisão aborda também a legitimidade da reclamante. Reconhece que esta tem, de facto, um interesse legítimo em solicitar uma investigação sobre factos relacionados com o tratamento de dados. Contudo, esclarece que este direito não se estende à exigência de instauração de processos sancionatórios ou à imposição de sanções específicas.

Consequentemente, a Audiência Nacional rejeita o recurso e mantém a atuação da Agência Espanhola de Proteção de Dados (AEPD), sem condenação em custas.

## Anulada uma sanção imposta a um membro de uma comissão de trabalhadores de um sindicato por reenviar e-mails corporativos para destinatários externos a essa comissão

A Audiência Nacional decidiu sobre um recurso administrativo interposto de uma resolução da AEPD de 30 de agosto de 2022, que aplicou uma coima de 2.000 euros por infração ao artigo 6.º, n.º 1 do RGPD, tal como definido no artigo 83.º, n.º 5 do RGPD e no artigo 72.º, n.º 1, alínea b) da Lei Espanhola de Proteção de Dados (LOPD-gdd).

A AEPD determinou que um membro da comissão de trabalhadores de um sindicato reencaminhou repetidamente e-mails com dados pessoais de outro membro da comissão (o reclamante), como o seu nome e endereço de e-mail profissional, para outros membros e não membros da comissão de trabalhadores, bem como para endereços de e-mail corporativos de sindicatos e outras organizações, sem autorização legal, sem o consentimento do reclamante e apesar da sua oposição expressa em diversas ocasiões.

Na sua decisão, a AEPD concluiu que tal constitui um tratamento ilícito de dados pessoais, considerando o tratamento dos dados pessoais do reclamante excessivo, uma vez que os e-mails em causa foram também enviados a pessoas externas à comissão de trabalhadores.

Contra esta decisão foi interposto recurso para a Audiência Nacional, tendo o recorrente argumentado que o correio eletrónico foi utilizado no âmbito da legislação laboral e no exercício de funções sindicais, e que todos os destinatários eram funcionários públicos ou representantes sindicais, os quais tinham acesso aos dados reclamados pelo reclamante através do Portal do Funcionário, tais como o endereço de correio eletrónico corporativo, o nome, a categoria profissional, a localização e o número de telefone do reclamante.

A Audiência Nacional reconheceu que um endereço de correio eletrónico corporativo constitui um dado pessoal quando se refere a um utilizador específico, em consonância com a própria doutrina da Agência no seu Parecer 0437/2010. Contudo, concluiu que não se podia ignorar o facto de o e-mail ter sido divulgado exclusivamente no seio da Administração Pública e de uma área organizacional específica, e que os destinatários eram funcionários públicos ou representantes sindicais que, estritamente falando, não podiam ser considerados terceiros alheios à informação enviada pela comissão de pessoal.

Além disso, o Tribunal sublinha que todos os destinatários tinham acesso ao Portal do Funcionário, o que significa que os dados divulgados já estavam publicados ou tinham sido autorizados para a sua divulgação, pelo menos nesse contexto, e, portanto, pertencem ao domínio público, nos termos do artigo 9.º, n.º 2, alínea e), do RGPD. Por todas estas razões, o Tribunal considera que o tratamento não pode ser considerado ilícito e, consequentemente, acolhe o recurso e anula a decisão da Agência Espanhola de Proteção de Dados (AEPD).

## Uma entidade destinatária não viola o direito à honra quando comprova a notificação prévia de pagamento antes de incluir os dados num registo de mora

Este acórdão do Supremo Tribunal analisa se a inclusão dos dados pessoais de um devedor num registo de solvabilidade patrimonial constitui uma intrusão ilícita no seu direito à honra quando se verifica o envio prévio de comprovativo de pagamento, mas não a prova conclusiva da sua receção.

O litígio decorre de uma ação judicial interposta por um particular contra uma empresa de gestão e aquisição de crédito, que tinha reportado os seus dados ao registo Asnef-Equifax devido a uma dívida decorrente de um contrato de serviço telefónico. O autor da ação argumentou que esta inclusão era ilegítima por não ter sido comprovada a receção efetiva do pedido prévio de pagamento, solicitando a remoção dos dados e uma indemnização por danos morais. Tanto o Tribunal de Primeira Instância como o Tribunal Provincial acolheram a ação, considerando insuficientes as provas apresentadas quanto à receção da notificação.

O Supremo Tribunal acolheu o recurso interposto pelo arguido e revogou as decisões anteriores. O Tribunal reiterou a sua doutrina consolidada de que a exigência de pedido

prévio não requer prova concludente da sua receção; basta a prova razoável de que o pedido foi devidamente entregue. Neste caso concreto, o pedido foi enviado por correio para a morada fornecida pelo devedor no contrato, a sua devolução não foi registada e não foi apresentada qualquer prova para lançar dúvidas sobre a sua entrega ao destinatário.

O Tribunal enfatizou ainda que a dívida era certa, vencida e exigível, facto não contestado na ação. Consequentemente, concluiu que não houve violação ilícita do direito à honra e julgou a ação improcedente na sua totalidade, condenando o autor no pagamento das custas processuais em primeira instância.

## O Supremo Tribunal afastou a violação do direito à honra pela inclusão de dados de dívida tributária obtidos em publicação oficial num registo de solvabilidade

O Supremo Tribunal deferiu o recurso interposto por uma empresa de serviços de informação de crédito, anulando a sentença do Tribunal Provincial de Madrid, que tinha declarado uma violação ilegal do direito de honra do demandante e condenado a empresa a pagar 4.000 euros a título de danos morais.

O litígio surgiu da inclusão dos dados do autor num registo de solvabilidade patrimonial, após a publicação no Boletim Oficial do Estado de um aviso de penhora por dívida tributária ao *Ayuntamiento* de Madrid. O registo manteve-se em vigor de fevereiro de 2017 a maio de 2021 e foi consultado por dois bancos, o que levou à recusa de um empréstimo à parte afetada.

A questão do recurso de cassação em análise pelo Supremo Tribunal era a de saber se os requisitos do artigo 29.º, n.º 2 e 4, da revogada Lei Orgânica n.º 15/1999 — pedido prévia de pagamento, aviso de inclusão e notificação posterior — são aplicáveis aos registos mencionados no n.º 1 do mesmo artigo, que são preenchidos com dados de fontes publicamente acessíveis. O Supremo Tribunal, reiterando a doutrina estabelecida nos seus acórdãos 434/2023 e 917/2025, concluiu que tais requisitos não são aplicáveis a estes registos, que se regem exclusivamente pelas disposições gerais da lei e dos seus regulamentos.

Consequentemente, o Tribunal acolhe o recurso, confirma a sentença do tribunal de primeira instância — que havia rejeitado a ação, considerando os dados verídicos e obtidos de fonte pública — e condena o autor no pagamento das custas do recurso.

## Supremo Tribunal reitera questões fundamentais relativas à inclusão de dados nos sistemas de informação de crédito

Este acordão analisa a legalidade do tratamento de dados pessoais nos sistemas de informação de crédito e o seu impacto no direito à honra, resolvendo um recurso de cassação interposto por uma entidade contra uma sentença que declarou a violação do direito da autora à honra devido à sua inclusão indevida no referido registo.

O Tribunal aborda três questões fundamentais relativas à proteção de dados:

- Princípio da qualidade dos dados: apenas as dívidas certas, vencidas e exigíveis podem ser registadas nos registos de solvabilidade. Esta inclusão foi ilícita porque a dívida não foi comprovada, uma vez que existiam discrepâncias entre o montante transferido e o certificado emitido pela entidade cedente.

- Pedido prévio de pagamento: o Tribunal reconhece a natureza funcional do pedido, mas estabelece que este perde relevância quando o devedor já consta de registos de mora devido a inclusões anteriores de outras entidades.

- Regime indemnizatório: distingue-se entre a violação do RGPD (que exige a prova de danos, nos termos do artigo 82.º, n.º 1 do RGPD e do Acórdão C-300/21 do TJUE) e a violação do direito à honra, em que se aplica a presunção legal de dano prevista no Artigo 9.º, n.º 3 da Lei Orgânica 1/1982.

A decisão acolhe parcialmente o recurso e reduz a indemnização de 7.000 € para 3.000 €.

## Anulada coima por tratamento ilícito de dados relacionado com uma dívida de cartão de crédito, mas confirmada coima por violação do direito de acesso

O acórdão acolhe parcialmente um recurso contencioso administrativo interposto por uma entidade de cobrança de dívidas contra uma decisão da AEPD que tinha imposto duas sanções por violação do RGPD no contexto de uma cobrança de dívida de cartão de crédito. A Audiência Nacional anulou a coima de 30.000 euros por alegado tratamento ilícito de dados (artigo 6.º, n.º 1 do RGPD) e manteve a coima do mesmo valor por negligência no cumprimento do direito de acesso (artigo 15.º do RGPD).

O caso teve origem numa reclamação de uma consumidora relativa a uma dívida que lhe era cobrada num cartão de crédito cuja contratação alegava desconhecer. A Audiência Nacional considerou haver provas suficientes de que o contrato tinha sido celebrado por telefone em outubro de 2000 (apesar da ausência de gravação da chamada ou de um contrato assinado), relevando a existência de dados pessoais da titular, a utilização do cartão até 2004, pagamentos subsequentes referenciados ao número da transação e a notificação da cessão do crédito em 2008, à qual a interessada não se opôs. Com base nisto, o Audiência Nacional concluiu que o tratamento dos dados era justificado pela execução do contrato (artigo 6.º, n.º 1, alínea b) do RGPD) e que a titular dos dados tinha dado o seu consentimento inequívoco. Por conseguinte, o tratamento dos dados foi considerado lícito.

Contudo, a Audiência Nacional manteve a sanção por infração ao artigo 15.º do RGPD, uma vez que a reclamante apenas atendeu ao pedido de acesso aos dados depois de a parte lesada ter apresentado uma reclamação à AEPD, sem demonstrar diligências prévias adequadas ou cumprimento do prazo legalmente estabelecido. A decisão reitera a obrigação de satisfazer o exercício dos direitos e de responder no prazo de um mês com informações claras, acessíveis e rastreáveis, em conformidade com os artigos 12.º e 15.º do RGPD.

## Confirmada a legalidade do tratamento de dados pessoais no registo de solvabilidade da ASNEF

O Supremo Tribunal indeferiu o recurso interposto por uma pessoa singular contra a decisão da Audiência Provincial de Madrid, que confirmou a legalidade da inclusão dos seus dados pessoais no registo da ASNEF a pedido de uma instituição de microcrédito.

O caso tem origem num microcrédito de 200 euros formalizado eletronicamente em dezembro de 2017. Perante o incumprimento, o mutuante enviou 22 mensagens de correio eletrónico de reclamação e uma carta postal — devolvida com a indicação "desconhecido" — antes de inscrever os dados na ASNEF, em março de 2018. A mutuária também não apresentou qualquer oposição no processo de injunção subsequente, que culminou num despacho de execução.

Do ponto de vista da proteção de dados, o Tribunal examina, em primeiro lugar, o princípio da qualidade dos dados, apreciando uma dívida certa, vencida e exigível, comprovada pela documentação contratual e pela conduta processual da devedora. Em segundo lugar, no que respeita ao pedido de pagamento prévio, reitera a sua doutrina consolidada sobre a sua natureza funcional: trata-se de uma salvaguarda destinada a impedir a inclusão de pessoas que deixaram de pagar por mero descuido ou erro, sem que essa informação seja relevante para a avaliação da sua solvabilidade. Neste caso, o Tribunal afasta qualquer efeito surpresa, tendo em conta a natureza do contrato, a existência de registos anteriores na ASNEF relativos a dívidas a outras duas entidades e a inação da parte afetada face às reclamações. Por conseguinte, quaisquer vícios formais na comprovação do pedido não constituem, por si só, um tratamento ilícito. Por fim, rejeita o argumento de que o princípio da minimização previsto no artigo 5.º, n.º 1, alínea c) do RGPD impede a inclusão de pequenas dívidas, uma vez que uma interpretação contrária excluiria do sistema os devedores que incumpriram reiteradamente pequenas obrigações.

## Declara-se que o direito à proteção de dados de uma trabalhadora foi violado quando o seu nome e salário foram divulgados numa carta de despedimento dirigida ao seu cônjuge

O Tribunal Superior de Justiça das Canárias declarou uma violação do direito fundamental à proteção de dados de uma funcionária de uma cadeia de supermercados O litígio resultou de uma carta de despedimento dirigida ao companheiro da trabalhadora, também funcionário da mesma cadeia, na qual, para justificar o recebimento de um complemento salarial indevido, a empresa incluiu o nome e o salário da funcionária como termo de comparação, já que ambos trabalhavam o mesmo número de horas. A empresa foi condenada a indemnizá-la em 7.500 euros.

O tribunal reconhece o legítimo interesse comercial no exercício da autoridade disciplinar e na justificação de despedimentos, mas considera desproporcional a divulgação de dados pessoais sem o consentimento do titular dos dados. Para atingir o mesmo objetivo, a comparação poderia ter sido feita sem mencionar uma pessoa específica, uma medida mais moderada que teria sido igualmente eficaz. Bastaria referir outro funcionário na mesma função ou utilizar dados anonimizados. A análise é realizada à luz dos artigos 5.º, n.º 1 e 6.º, n.º 1 do RGPD, enfatizando a exigência de proporcionalidade no tratamento de dados no âmbito laboral.

# Contacte os nossos profissionais


**Alejandro Padín**
Sócio - Madrid
alejandro.padin@garrigues.com

**Luisa Cyrne**
Associada principal· Lisboa
luisa.cyrne@garrigues.com

**Álvaro Blanco**
Associado sénior · Madrid
alvaro.blanco@garrigues.com

**Andrea Ugalde**
Associada - Bilbau
andrea.ugalde@garrigues.com

**Garazi Tomás**
Associada - Bilbau
garazi.tomas@garrigues.com

**Ignacio Suárez**
Associado - Madrid
ignacio.suarez@garrigues.com

**Laia Llambrich**
Associada - Bilbau
laia.llambrich@garrigues.com

**Franco Muschi**
Sócio· Lima
franco.muschi@garrigues.com

**Adrián León**
Associado sénior · Alicante
adrian.leon@garrigues.com

**Mariana Ubidia**
Associada sénior · Lima
mariana.ubidia@garrigues.com

**Carina Casadesús**
Associada · Barcelona
carina.casadesus@garrigues.com

**Iciar Velasco**
Associada · Madrid
iciar.velasco@garrigues.com

**Javier Enebral**
Associado - Madrid
javier.enebral@garrigues.com

**Marta Sabio**
Associada · Barcelona
marta.sabio@garrigues.com


Mais informações:
**Economia de Dados, Privacidade e Cibersegurança**

GARRIGUES


Plaza de Colón, 2 - 28046 Madrid
**T** +34 91 514 52 00

info@garrigues.com
**garrigues.com**


**Siga-nos em:**