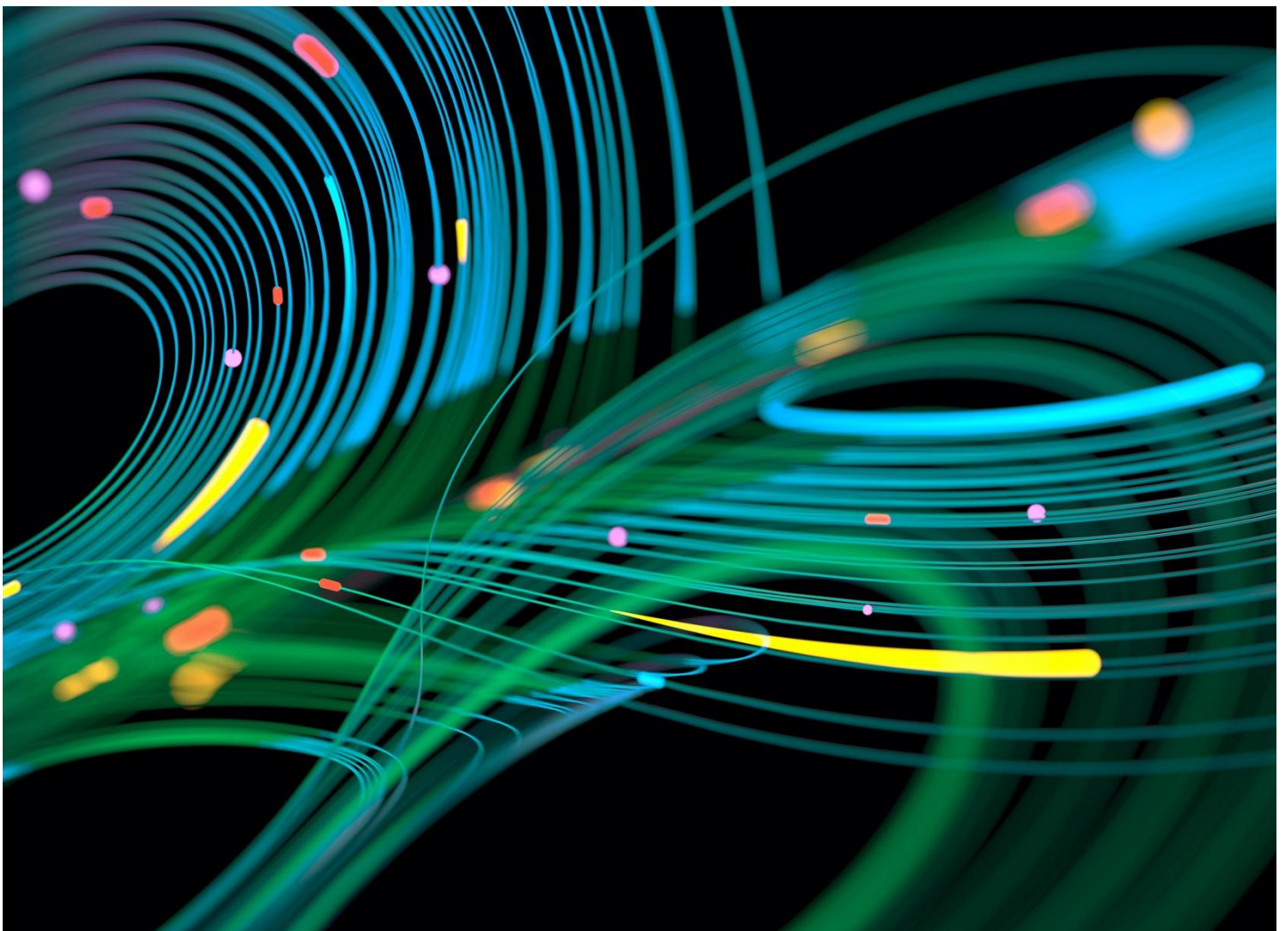


GARRIGUES

Newsletter Economia de Dados, Privacidade e Cibersegurança

Fevereiro de 2026

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



A UE promove em 2026 uma profunda reconfiguração da economia digital, propondo alterações na regulamentação de IA, dados e plataformas



[Alejandro Padín Vidal](#)

2026 apresenta-se repleto de reformas que irão redefinir a IA, a privacidade e os mercados digitais na UE. A agenda regulatória caminha para uma maior transparência, supervisão reforçada e novas obrigações para plataformas, fornecedores de tecnologia e empresas que tratam dados ou dependem de serviços digitais. Um ano fundamental para antecipar riscos, adaptar processos e fortalecer a estratégia digital empresarial.

Na economia digital, 2026 promete ser, mais uma vez, um ano de desenvolvimentos inovadores e desafios regulatórios significativos.

Inteligência artificial

Em relação à inteligência artificial, 2026 será o ano em que veremos a consolidação definitiva ou o adiamento da aplicação do Regulamento de Inteligência Artificial (RIA). A Comissão Europeia publicou [uma proposta de regulamento](#) que, se adotada, introduziria diversas alterações significativas ao RIA, incluindo uma que afetaria o prazo de implementação obrigatório de toda a regulamentação relativa às obrigações aplicáveis aos fornecedores e aos responsáveis pela implementação de sistemas de alto risco. [Neste link](#) pode consultar a publicação correspondente.

Simplificação do acervo digital europeu

No próximo ano de 2026, assistiremos também a intensos debates sobre alguns dos conceitos estruturais da regulamentação da economia digital, como o próprio conceito de "dados pessoais" ou o conceito de "pseudonimização". Esta é consequência de outra [proposta de regulamento](#) da Comissão Europeia, desta vez sob o nome genérico de "simplificação do acervo digital europeu", que propõe a alteração de importantes regulamentos, como o Regulamento Geral sobre a Proteção de Dados (RGPD), a Diretiva NIS 2 e a Lei de Proteção de Dados (*Data Act*), em que seriam integrados, para além da revogação de outras normas relacionadas, como o Regulamento de Governança de Dados

(*Data Governance Act*) ou a Diretiva relativa aos dados abertos e à reutilização de informações do setor público.

Privacidade

Os princípios básicos consagrados nos regulamentos de proteção de dados da União Europeia estão a ser revistos, tanto na sequência de desenvolvimentos jurisprudenciais (por exemplo, pelo questionamento da doutrina tradicional e absoluta do conceito de dados pessoais, como se verificou no acórdão do TJEU no processo [SRB vs EDPS](#)) como devido a propostas de alterações legislativas já referidas, incluídas no pacote Omnibus e noutros desenvolvimentos regulamentares. Embora o objectivo seja simplificar e racionalizar a aplicação das normas, verifica-se resistência por parte dos defensores dos direitos fundamentais, o que provavelmente levará a intensos debates doutrinários e regulamentares, cujo resultado é actualmente difícil de prever.

Numa perspetiva internacional, e com foco nas jurisdições onde a Garrigues está presente, o Chile enfrenta todo o processo de adaptação à nova lei de proteção de dados. Deste modo, as empresas chilenas ou com negócios neste país são obrigadas a realizar os trabalhos necessários para cumprir o regulamento antes da sua aplicação obrigatória.

Regulamento dos Serviços Digitais (DSA)

Em 2026, a aplicação efetiva do Regulamento dos Serviços Digitais (DSA) continuará a intensificar-se. Este regulamento está a consolidar um quadro homogéneo na UE para a responsabilidade e obrigações de diligência dos prestadores de serviços intermediários (alojamento, redes sociais, *marketplaces*, motores de busca, etc.). O ano será marcado por um aumento das ações de supervisão, dos critérios interpretativos e da resolução de procedimentos (incluindo medidas corretivas), especialmente no que diz respeito às obrigações de transparência, à gestão de conteúdos ilícitos, à rastreabilidade dos comerciantes em *marketplaces*, aos sistemas de notificação e atuação e aos mecanismos de reclamação e *redress*. No caso das grandes plataformas e motores de busca, a exigência de avaliações e mitigação de riscos sistémicos (por exemplo, proteção infantil, efeitos algorítmicos, desinformação, riscos para a segurança e saúde pública) será particularmente relevante, assim como a transparência da publicidade e a fiscalização de práticas como padrões de conceção enganosos.

Em Espanha, a supervisão da DSA articula-se em torno da CNMC, coordenadora dos serviços digitais. No entanto, a implementação efetiva do quadro nacional (incluindo o regime de sanções e a plena operacionalização da supervisão) permanece intimamente ligada aos processos normativos internos e à alocação de recursos. Deste modo, prevê-se que 2026 seja um ano de consolidação institucional e de aumento gradual das ações de supervisão e da coordenação com a Comissão Europeia.

Regulamento dos Mercados Digitais (DMA)

Paralelamente, a aplicação prática do Regulamento dos Mercados Digitais (DMA) será consolidada em 2026. Este regulamento visa garantir mercados digitais abertos e efetivamente competitivos através de obrigações específicas para os *gatekeepers*. O foco passará da simples designação destes operadores para a avaliação das suas medidas de conformidade e a tomada de decisões sobre práticas-chave que afetam a estrutura do mercado, como a autopreferência, as restrições à liberdade comercial dos utilizadores empresariais, a interoperabilidade e as condições de acesso a ecossistemas fechados (*app stores* e sistemas operativos) e a utilização de dados. Prevê-se que este processo seja acompanhado por um aumento da litigância e pela necessidade de coordenar a análise regulatória com as áreas da concorrência, defesa do consumidor e proteção de dados.

O mais tardar em maio de 2026, a Comissão Europeia apresentará o seu primeiro relatório sobre a aplicação do Regulamento dos Mercados Digitais (RMD) às restantes instituições da União Europeia. Uma das questões centrais que a Comissão Europeia terá de abordar neste relatório é se, e em que medida, o regulamento se aplica à inteligência artificial (IA).

Em particular, a Comissão Europeia poderá considerar a inclusão da IA nas categorias existentes de “serviços essenciais de plataforma” (*core platform services*) ou, se necessário, propor definições novas ou modificadas para abranger ferramentas e serviços de IA. De igual modo, a Comissão Europeia analisará a forma como as obrigações substantivas da DMA se aplicam à IA e se são necessárias alterações legislativas para o efeito.

Por razões de eficiência e celeridade, espera-se que a Comissão Europeia dê preferência a soluções que não exijam uma reforma legislativa.

e-IDAS e identidade digital

Outra área em que se esperam desenvolvimentos significativos em 2026 é a identidade digital. Este ano, prevê-se a conclusão do desenvolvimento das especificações técnicas para a implementação real e efetiva da Carteira de Identidade Digital Europeia (*EU ID Digital Wallet*), que representará um marco nos mecanismos de identificação oficial das pessoas na União Europeia, uma vez que permitirá aos utilizadores ter uma carteira digital sob a forma de uma aplicação móvel com todas as suas credenciais oficiais (cartão de cidadão, carta de condução, cartões de saúde, cartões de biblioteca ou universidade, títulos académicos, etc.).

Cibersegurança

Esperamos também que 2026 seja o ano em que a lei que transpõe a Diretiva NIS 2 para Espanha seja aprovada e publicada, não só devido ao atraso que já estamos sofrer relativamente à data obrigatória para a entrada em vigor desta norma crucial (que deveria ter sido aprovada antes de outubro de 2024), mas também devido à sua extraordinária importância para alcançar um nível mais elevado de segurança nas redes e sistemas de um grande número de empresas em Espanha, pertencentes a diversos setores da economia. O trabalho de adaptação necessário em muitas empresas representa um desafio operacional significativo que deve ser enfrentado sem demora.



Atualidade

A Comissão Europeia impõe à X a primeira coima por aplicação do ‘Digital Services Act’ (DSA) a uma VLOP

A Comissão Europeia investigou a plataforma X (anteriormente Twitter), classificada como uma “*very large online platform*” (VLOP), por potenciais violações das obrigações reforçadas impostas pelo Regulamento dos Serviços Digitais (DSA), em particular no que diz respeito ao desenho de interfaces, à transparência da publicidade e ao acesso a dados para os investigadores.

A Comissão [conclui](#) que a X infringiu várias disposições do DSA e aplicou uma coima de 120 milhões de euros, a primeira sanção adotada ao abrigo do novo regime de sanções do referido regulamento.

Em primeiro lugar, considera a conceção do sistema de “verificação azul” enganador, uma vez que permite aos utilizadores obter o selo de conta verificada mediante o pagamento de uma taxa de subscrição sem verificação efetiva da identidade, dificultando a avaliação da autenticidade das contas e aumentando os riscos de falsificação de identidade e fraude.

A Comissão apreciou também incumprimentos das obrigações de transparência da publicidade devido à inexistência de um repositório de anúncios em conformidade com o DSA e pelo incumprimento do dever de proporcionar aos investigadores acreditados o acesso a dados públicos, através da imposição de restrições contratuais indevidas.

A decisão confirma que o DSA não só regula os conteúdos ilegais, mas também a conceção das plataformas, a transparência e a

responsabilização das grandes plataformas digitais.

O CEPD submete a consulta pública as recomendações 2/2025 sobre a base jurídica para exigir a criação de contas de utilizador em sites de comércio eletrónico

O Comité Europeu para a Proteção de Dados (CEPD) publicou as [recomendações 2/2025](#) sobre a base jurídica para exigir a criação de contas de utilizador em sites de comércio eletrónico para as submeter a consulta pública. O documento analisa a prática cada vez mais comum de exigir que os utilizadores se registem para aceder a ofertas ou realizar compras *online* e conclui que, em geral, esta exigência não está em conformidade com o RGPD se não existir uma base jurídica clara e suficiente.

Como princípio geral, o CEPD salienta que os utilizadores devem poder comprar ou interagir com uma plataforma de comércio eletrónico sem terem de criar uma conta obrigatória, recomendando opções como a compra como visitante ou a criação voluntária de contas, em conformidade com os princípios da proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD).

Relativamente aos fundamentos jurídicos do artigo 6.º do RGPD, o CEPD esclarece que:

- i. A celebração de um contrato só pode justificar uma conta obrigatória quando esta seja estritamente necessária para a prestação do serviço, como acontece nos serviços de subscrição ou nas relações

contínuas, mas não nas simples vendas pontuais.

- ii. A existência de uma obrigação legal apenas permitiria exigir uma conta quando um regulamento o exigisse expressamente, um cenário atualmente pouco comum no comércio eletrônico.
- iii. O interesse legítimo não é, geralmente, suficiente para justificar a obrigatoriedade de criação de contas quando existem alternativas menos intrusivas que não infringem os direitos e liberdades dos utilizadores.

O CEPD identifica também riscos significativos associados à criação obrigatória de contas, como o tratamento excessivo de dados pessoais, períodos de conservação de dados mais longos e aumento dos riscos de segurança e acesso não autorizados.

Em conclusão, o CEPD afirma que a criação obrigatória de contas deve ser a exceção, e não a regra, e só será compatível com o RGPD quando passar por uma análise rigorosa de necessidade e proporcionalidade, devendo os responsáveis pelo tratamento de dados oferecer, sempre que possível, alternativas que respeitem mais a privacidade do utilizador.

A Agência Nacional de Cibersegurança do Chile aprova a lista final do primeiro processo de qualificação para operadores de importância vital

A Agência Nacional de Cibersegurança do Chile (ANCI) aprovou, através da Resolução isenta n.º 87, a lista final do primeiro processo de qualificação para operadores de importância vital (OIV), de acordo com o procedimento estabelecido pela Lei n.º 21.663, Lei-Quadro de Cibersegurança, e o seu Regulamento, após consulta pública e avaliação técnica multissetorial, consolidando um marco fundamental no novo quadro de cibersegurança chileno.

O processo de qualificação consistiu numa avaliação em duas fases: dependência de redes e sistemas informáticos e impacto significativo na segurança, ordem pública, continuidade dos serviços essenciais e funções do Estado, ponderados de acordo com os

critérios do regulamento. A lista abrange eletricidade, telecomunicações, infraestruturas e serviços digitais, serviços bancários/financeiros/meios de pagamento, prestadores de serviços de saúde institucionais, empresas estatais e entidades da Administração Pública, com base em relatórios setoriais e consulta pública.

A resolução estabelece obrigações reforçadas de gestão de riscos, continuidade e resiliência para os OIV e prevê próximas fases para os restantes setores, consolidando uma abordagem sistémica e gradual para a proteção da infraestrutura digital crítica.

A lista pode ser consultada no seguinte [link](#).

A AESIA publica guias práticos para facilitar o cumprimento do Regulamento Europeu da Inteligência Artificial (RIA)

A Agência Espanhola de Supervisão da Inteligência Artificial (AESIA), um organismo público dependente do Ministério para a Transformação Digital e da Administração Pública, publicou um conjunto de [16 guias práticos](#) elaborados para apoiar as organizações públicas e privadas na compreensão, implementação e cumprimento do Regulamento Europeu da Inteligência Artificial (RIA/AI Act).

Estes guias, que resultam do ambiente regulamentar experimental espanhol para a IA, dirigem-se tanto a PME e *startups* como a grandes empresas que desenvolvem ou implementam sistemas de IA de alto risco, com recomendações alinhadas com os requisitos regulamentares europeus e aguardam normas harmonizadas.

As publicações não são vinculativas e não substituem os regulamentos aplicáveis, mas fornecem orientações operacionais detalhadas sobre obrigações complexas, ajudando as entidades a organizar as suas estratégias de conformidade antes da entrada em vigor progressiva dos requisitos do *AI Act*, tendo em vista especialmente agosto de 2026.

Listagem de guias publicados:

1. Guia de introdução ao regulamento de IA

2. Guia prático e exemplos para a compreensão do Regulamento da IA
3. Guia de Avaliação da Conformidade
4. Guia do Sistema de Gestão da Qualidade
5. Guia de Gestão de Riscos
6. Guia de Vigilância Humana
7. Guia de Dados e Governança de Dados
8. Guia de Transparência
9. Guia de Precisão
10. Guia de Solidez
11. Guia de Cibersegurança
12. Guia de Registos
13. Guia de Vigilância Pós-comercialização
14. Guia de Gestão de Incidentes
15. Guia de Documentação Técnica
16. Manual de *checklist* de guias de requisitos (*checklists* e exemplos)

Estes guias estão estruturados em três blocos (introdutórios, técnicos e *checklist*) e constituem uma ferramenta prática para ajudar as organizações espanholas e de outros países da UE a adaptarem os seus sistemas de IA ao quadro europeu, com foco na inovação responsável e no respeito pelos direitos fundamentais.

Foi publicada a atualização da norma ISO 27701:2025 sobre gestão de informação de privacidade

A Organização Internacional de Normalização (ISO) [publicou](#) a nova ISO 27701:2025, uma atualização da norma internacional que amplia os requisitos e orientações para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de gestão de informação de privacidade (PIMS).

A norma, que complementa a ISO 27001 sobre segurança da informação, reforça a integração entre a segurança e a proteção de dados pessoais, estabelecendo orientações adaptadas ao contexto do Regulamento Geral de Proteção de Dados (RGPD) e de outros quadros internacionais.

A publicação da versão de 2025 atualiza os controlos, a terminologia e as referências normativas, alinhando-os com as versões mais recentes das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, consolidando assim o seu papel de referência para as organizações que procuram certificar a gestão da privacidade dos seus sistemas de segurança.

Artigo no blogue da AEPD: equilibrar os direitos fundamentais quando está em causa a proteção da criança

A AEPD publicou um [artigo no seu blog](#) em que reforça o conceito do "interesse superior da criança", consagrado no artigo 24.º, n.º 2 da Carta dos Direitos Fundamentais da União Europeia e citado em várias decisões do Tribunal de Justiça da União Europeia, como no processo [C-230/21](#).

Na área da proteção das crianças online, defende-se frequentemente um equilíbrio entre o interesse superior da criança e o direito à proteção de dados. No entanto, a AEPD conclui que “esta falsa dicotomia visa, na verdade, expressar que os direitos fundamentais devem ser equilibrados com os interesses comerciais dos atores que operam no ecossistema digital”, acrescentando que “esta é uma falsa escolha que não deve ser feita, tal como não deve ser aceite a falsa escolha entre segurança e privacidade, expressa no passado em diferentes cenários”.

Ao ponderar os interesses das crianças, a AEPD indica que “o interesse superior da criança e o direito à proteção de dados estão do mesmo lado da balança; são complementares e, por isso, não devem ser equilibrados, nem um deve ser comprometido em favor do outro”. Portanto, com este artigo da AEPD, conclui-se que o equilíbrio de direitos fundamentais (como o direito à privacidade), utilizando os conceitos de idoneidade, necessidade e proporcionalidade, não tem lugar no âmbito da proteção da criança.

O Comité Europeu para a Proteção de Dados (CEPD) e a Comissão Europeia aprovaram orientações conjuntas sobre a interação entre o Regulamento dos Mercados Digitais (DMA) e o Regulamento Geral sobre a Proteção de Dados (RGPD).

Em 9 de outubro de 2025, o CEPD e a Comissão Europeia publicaram as [primeiras orientações](#) para facilitar a aplicação consistente do DMA e do RGPD, proporcionar maior segurança jurídica e simplificar o cumprimento para utilizadores, beneficiários e indivíduos em geral.

Este primeiro guia visa harmonizar as interpretações e reduzir as dificuldades de cumprimento. Entre outros aspetos fundamentais, as orientações publicadas esclarecem os elementos que devem ser considerados para cumprir os requisitos de “escolha específica” e “consentimento válido” do Artigo 5.º, n.º 2 do DMA e do RGPD, permitindo a combinação ou utilização cruzada lícita de dados pessoais em serviços de plataforma essenciais. O documento aborda ainda questões relacionadas com a distribuição de aplicações e lojas de terceiros, portabilidade de dados, pedidos de acesso a dados e interoperabilidade de serviços de mensagens.

O texto final, que integrará os contributos recebidos durante a consulta pública lançada pelo CEPD e pela Comissão, será elaborado em conjunto por ambas as entidades.

O sistema de entradas e saídas (SES) da UE entra em funcionamento

Após a entrada em vigor do sistema de entradas e saídas (SES) da UE, no dia 12 de outubro de 2025, o Comité de Supervisão Coordenada (CSC) [incluiu-o](#) no seu âmbito de aplicação.

O SES é um sistema informático de grande escala desenvolvido pela UE para prevenir a migração irregular e melhorar a segurança no Espaço Schengen. Prevê-se que venha a substituir gradualmente o sistema de carimbo de passaportes nas fronteiras exteriores do

Espaço Schengen, com o objetivo de otimizar os processos fronteiriços.

Este sistema regista os cidadãos não pertencentes ao Espaço Schengen que viajam com vistos de curta duração ou isentos de visto, incluindo os dados pessoais dos seus documentos de viagem, como o nome, a data e o local de nascimento. Regista também as datas de entrada e saída dos viajantes, além de dados biométricos, como imagens faciais e impressões digitais. As autoridades que tratam dados pessoais no SES — como as autoridades fronteiriças, os serviços de imigração e, em determinadas circunstâncias, as forças policiais — devem garantir que as pessoas podem solicitar facilmente o acesso aos seus dados e exercer os seus direitos ao abrigo do RGPD.

Prevê-se que o SES esteja completamente operacional até 10 de abril de 2026, altura em que o sistema será utilizado em todas as passagens de fronteira para todos os cidadãos de países terceiros que cumpram os requisitos e possuam passaportes biométricos.

O Comité Europeu para a Proteção de Dados incidirá a sua quinta ação coordenada no cumprimento das obrigações de transparência

O CEPD [anunciou](#) que a sua quinta ação coordenada de controlo se centrará na verificação do cumprimento das obrigações de transparência e informação estabelecidas nos artigos 12.º, 13.º e 14.º do RGPD, que garantem o direito das pessoas singulares a serem informados sobre o tratamento dos seus dados pessoais..

Neste tipo de ações, o CEPD seleciona um tema prioritário e as autoridades nacionais de proteção de dados conduzem investigações paralelas e coordenadas. Posteriormente, o comité compila as conclusões e formula recomendações comuns ou medidas de acompanhamento a nível nacional e europeu.

As ações anteriores centraram-se em aspetos-chave, como a utilização de serviços na nuvem no setor público (2023), o papel do encarregado da proteção de dados (2024) e o direito de acesso (2025). A nova iniciativa será desenvolvida ao longo de 2026 e complementa

a ação em curso sobre o direito ao apagamento (artigo 17.º do RGPD), cujo relatório final será publicado nos próximos meses.

As transferências de dados UE-Reino Unido poderão manter-se sem garantias adicionais, embora com vigilância quanto a eventuais riscos futuros

Segundo a AEPD, em [comunicado de 23 de outubro](#), o Comité Europeu para a Proteção de Dados (CEPD) emitiu um parecer favorável à proposta da Comissão Europeia de prorrogar a decisão de adequação do Reino Unido até dezembro de 2031. Esta prorrogação permitirá às organizações europeias continuar a transferir dados pessoais para o Reino Unido sem necessidade de salvaguardas adicionais, uma vez que o CEPD considera o seu quadro de proteção de dados essencialmente equivalente ao europeu.

O CEPD avalia positivamente a continuidade e a estabilidade dos fluxos de dados internacionais, assim como a harmonização contínua entre os regimes do Reino Unido e da Europa, mesmo após as recentes reformas legislativas no Reino Unido. No entanto, alerta a Comissão para vários riscos que exigem controlo ativo, incluindo os efeitos da Lei de Revogação do Direito da UE (REUL) e o seu potencial impacto na coerência normativa, a expansão dos poderes do governo britânico que poderá reduzir o controlo parlamentar em áreas-chave e as implicações relativas ao acesso do governo aos dados, à encriptação e às isenções por motivos de segurança nacional.

Em conclusão, embora o CEPD apoie a prorrogação, insiste na necessidade de a Comissão Europeia manter uma vigilância contínua sobre as alterações legislativas do Reino Unido para garantir que o nível de proteção se mantém equivalente durante todo o período da decisão de adequação.

Impostas medidas corretivas à Microsoft por tratamento de dados pessoais de menores na Áustria

A autoridade austríaca de proteção de dados decidiu, no dia 8 de outubro, que a Microsoft rastreou ilegalmente os estudantes que utilizavam o seu software educativo, negando-lhes o acesso aos seus dados e utilizando *cookies* sem consentimento.

A [decisão](#) da autoridade austríaca (DSB) foi a resposta a uma queixa apresentada em 2024. O denunciante, pai de um menor cuja escola utiliza o software da Microsoft, informou a autoridade austríaca que nem ele nem o seu filho tinham consentido a instalação de *cookies* e que não conseguia obter informações sobre a forma como os dados do seu filho estavam a ser utilizados.

A DSB constatou a existência de violações do direito de acesso e de informação e determinou a implementação de determinadas medidas corretivas. Mais concretamente, entre outras questões, determina que as informações fornecidas aos utilizadores sejam complementadas de acordo com o artigo 13.º do RGPD e que os dados tratados de menores com origem em *cookies* não técnicos sejam revistos e, quando aplicável, eliminados no prazo de dez semanas.

A 'Global Privacy Assembly' aprova três novas resoluções centradas na inteligência artificial e na educação digital

A *Global Privacy Assembly (GPA)*, que reúne autoridades de proteção de dados de todo o mundo, adotou três novas [resoluções](#) relevantes na sua 47ª sessão anual, realizada recentemente na Coreia do Sul, duas das quais se focam diretamente na inteligência artificial.

A primeira aborda a utilização de dados pessoais no treino de modelos de IA, salientando que esses dados só podem ser utilizados se tiverem sido obtidos legalmente e de acordo com os princípios do RGPD, reiterando que a disponibilidade pública não equivale a uma utilização legítima.

A segunda resolução centra-se na supervisão humana eficaz das decisões automatizadas, definindo as funções de supervisão, os requisitos de formação e a obrigação de documentar as decisões tomadas com o apoio de sistemas de IA.

Por fim, a terceira resolução refere-se à educação digital e à cidadania responsável, recomendando a criação de conteúdos educativos sobre os direitos de proteção de dados e protocolos de acessibilidade para as instituições de ensino, de forma a promover uma cultura digital inclusiva e segura.

A Agência lança a revista científica “Privacidad, Innovación y Tecnología” e convida autores para publicarem na primeira edição

A AEPD lançou a [revista científica “Privacidad, Innovación y Tecnología” \(PIT\)](#), um novo fórum académico dedicado à reflexão, análise e divulgação de conhecimentos especializados sobre privacidade, proteção de dados e o impacto das tecnologias disruptivas — especialmente a inteligência artificial — nos direitos fundamentais.

A criação desta revista reforça a missão institucional da Agência e procura consolidar um ecossistema de investigação rigoroso e útil para todos os setores envolvidos. A PIT inspira-se nos valores da independência, inovação, cooperação e excelência, e foi concebida para fortalecer a colaboração entre a Agência, a academia, o setor empresarial e a sociedade, promovendo a transferência de conhecimento e a análise interdisciplinar.

A AEPD abrirá o período de submissão de artigos para as próximas edições da revista, aceitando contribuições originais em espanhol ou inglês, que serão avaliadas através de uma revisão duplo-cego por pares externos. A publicação da primeira edição está prevista para abril de 2026, sob uma licença CC BY-NC, garantindo o acesso aberto e a transparência.

A revista PIT pretende também servir como observatório de boas práticas, casos de utilização e propostas regulatórias, demonstrando que a inovação tecnológica e a conformidade regulamentar são compatíveis e necessárias para um desenvolvimento ético e sustentável.

Resoluções

A AEPD aplicou uma sanção à AENA relativamente a um sistema de reconhecimento biométrico

Neste caso, a AENA tinha lançado um projeto piloto de reconhecimento biométrico de passageiros para controlar o fluxo de passageiros nos aeroportos. Esta medida, tal como consta na [resolução](#) emitida pela AEPD, era opcional, o que significa que os passageiros podiam continuar a identificar-se utilizando os métodos tradicionais.

Durante o lançamento deste projeto, a AENA submeteu consultas preliminares à AEPD, depois de ter realizado as respetivas avaliações de impacto do tratamento de dados pretendido.

Esta resolução é importante porque contém um resumo dos critérios da AEPD relativos ao tratamento de dados biométricos por parte dos responsáveis pelo tratamento, cuja viabilidade, em termos gerais, tem sido questionada de acordo com os critérios mais recentes da autoridade de controlo. A este propósito, é de salientar a análise da AEPD sobre os critérios de necessidade e proporcionalidade do tratamento de dados, em que reitera que: (i) a utilidade ou conveniência do tratamento não legitima a escolha de um sistema “agressivo” em relação aos direitos e liberdades das pessoas; e (ii) os dados biométricos são dados especialmente protegidos, pelo que qualquer tratamento deste tipo de dados deve ser precedido de análises exaustivas do impacto do tratamento, assim como acompanhado da implementação de garantias suficientes.

É relativamente a estas avaliações de impacto que a AEPD aplica a sanção pecuniária (10.043.002 euros) à AENA, por considerar que não foram suficientemente completas ou

detalhadas, exigindo um maior rigor, especialmente no que diz respeito à análise da necessidade e proporcionalidade do tratamento.

Por conseguinte, esta resolução não só define os critérios da AEPD relativamente ao tratamento de dados biométricos, como também sublinha a importância da realização de avaliações de impacto detalhadas e abrangentes. O incumprimento desta obrigação pode, por si só, ter consequências significativas.

Aplicadas duas coimas milionárias a uma empresa telefónica por incidente de segurança

Nesta [resolução](#) da AEPD são aplicadas duas coimas milionárias a uma empresa telefónica por violações do Artigo 5.º, n.º 1, al. f) do RGPD, referente ao princípio da confidencialidade dos dados (2.500.000 euros), e do Artigo 32.º do RGPD, referente às medidas de segurança (1.500.000 euros).

Neste caso, de acordo com a resolução, depois de receberem uma notificação do responsável pelo tratamento de dados a informar sobre um incidente de segurança que resultou na perda de confidencialidade dos seus dados pessoais, vários clientes apresentaram reclamações à AEPD.

Para além da avaliação das medidas específicas implementadas pelo responsável pelo tratamento de dados, o aspeto mais significativo desta resolução é a sua análise da ocorrência simultânea das duas infrações acima referidas. A AEPD faz esta apreciação sem atender às alegações do responsável de que a imposição de coimas por estas duas

disposições relacionadas entre poderia violar o princípio *non bis in idem*. A AEPD também não releva a ocorrência de um concurso instrumental nem a violação do princípio da especialidade, reafirmando assim a sua posição anterior de que ambas as infrações podem ser sancionadas em simultâneo relativamente ao mesmo incidente.

Esta resolução contém uma compilação atualizada dos argumentos apresentados pela AEPD a este respeito e serve como uma recordatória clara do nível de diligência exigido aos responsáveis pelo tratamento de dados tanto antes (na adoção de medidas de segurança, por exemplo) como depois de um incidente (na sua gestão).

Instituição financeira sancionada por não garantir a rastreabilidade e segurança de dados pessoais no envio de documentação através da sua empresa de correio

A AEPD sancionou uma [instituição financeira](#) por violar o artigo 32.º do RGPD ao não implementar medidas técnicas e organizativas adequadas para garantir a segurança do tratamento de dados pessoais durante a sua relação contratual com uma empresa de entregas expresso responsável pela recolha de documentação de clientes. A resolução sublinha que a instituição, enquanto responsável pelo tratamento dos dados, era obrigada a estabelecer mecanismos eficazes de rastreabilidade e alerta precoce para detetar e gerir potenciais violações de dados, para além da mera existência formal de contratos ou avaliações de impacto.

O argumento da instituição financeira quanto à diligência na seleção e controlo do seu subcontratante para o tratamento de dados foi rejeitado, tendo a AEPD salientado que a falta de controlo efetivo e a ausência de medidas específicas para a rastreabilidade dos envios constituem uma violação do seu dever de segurança. Além disso, salienta-se que a perda de dados pessoais constitui uma violação do direito fundamental de proteção de dados, independentemente de ter sido comprovado o acesso não autorizado por terceiros.

A sanção é graduada com base na gravidade da violação, no número de potenciais afetados e na natureza dos dados perdidos (incluindo números de documentos de identidade e dados bancários), sendo aplicada uma coima de 500.000 euros, reduzida para 400.000 euros em caso de pagamento voluntário. A resolução sublinha a obrigação proativa e permanente de adaptar as medidas de segurança ao nível de risco.

Uma universidade sancionada pela utilização de biometria em sistemas de ‘proctoring’

A AEPD decidiu [sancionar](#) uma universidade por tratar dados biométricos através de um sistema de monitorização com reconhecimento facial imposto aos estudantes sem oferecer alternativas.

A Agência declara a violação do artigo 9.º do RGPD (tratamento de categorias especiais de dados pessoais) pelo tratamento de dados biométricos sem base de legitimação ou exceção que o permita. Especificamente, determina que a autenticação individual utilizando padrões de geometria facial constitui tratamento de dados biométricos. A universidade argumentou que o reconhecimento facial era exigido pela Agência Nacional de Avaliação da Qualidade e Acreditação (ANECA) para prevenir fraudes académicas, mas a AEPD rejeita esta justificação, considerando que nenhuma regulamentação obriga a esse tratamento e que, em qualquer caso, as orientações da ANECA não têm fundamento jurídico suficiente para o autorizar.

No que respeita ao consentimento dado pelos estudantes, a Agência conclui que este não constitui um consentimento livre e esclarecido, uma vez que não existem alternativas equivalentes e existe um desequilíbrio de poder entre a instituição e os estudantes, análogo ao existente no âmbito laboral. Sublinha-se também que a universidade rejeitou aplicações que não exigiam dados biométricos. No entanto, a AEPD reconhece que, até à publicação do Guia de Biometria em novembro de 2023, existiam dúvidas razoáveis sobre este tipo de tratamento de dados e, por conseguinte, reduz o período sancionável a partir dessa data. É aplicada uma coima de 300.000 € por esta infração.

Além disso, a Agência sanciona a infração do artigo 5.º, n.º 1, alínea c), do RGPD (princípio da minimização), considerando que o sistema utilizado era desnecessariamente intrusivo, tendo em conta a existência de alternativas operacionais que não exigiam dados biométricos. A AEPD sublinha que o tratamento é desproporcionado, os meios utilizados não justificam o fim prosseguido e a escolha do sistema baseou-se em critérios de eficiência organizacional e não de proteção de dados. Neste caso, o período de infração não é reduzido, uma vez que é considerado contínuo desde a entrada em vigor do RGPD, sendo aplicada uma coima de 350.000 euros.

Fornecedor de energia multado em 200.000 € por cancelar o serviço do cliente errado

A AEPD [sancionou](#) um fornecedor de energia em 200.000 euros por violação do princípio da exatidão estabelecido no artigo 5.º, n.º 1, al. d) do RGPD durante o tratamento de uma alteração de fornecedor e de titularidade num contrato de fornecimento de eletricidade e gás.

O caso surge quando um terceiro contratou serviços de eletricidade e gás com a empresa sancionada em março de 2022. Durante este processo de contratação, o fornecedor associou erradamente os códigos CUPS (que identificam o ponto de fornecimento) do reclamante ao contrato desse terceiro. Como consequência, quando o terceiro cancelou o seu contrato, o fornecimento à residência do reclamante foi interrompido, deixando-o sem eletricidade ou gás durante dois dias.

A AEPD considera comprovado que a empresa não implementou as medidas necessárias para garantir a exatidão dos dados, como a verificação do código CUPS e da ligação do contratante ao ponto de fornecimento. A empresa argumentou que o erro se deveu a uma confusão relativamente ao endereço e às informações de identificação do contratante, chegando mesmo a invocar o conceito de "erro invencível". No entanto, a Agência rejeitou estas alegações, referindo que o fornecedor de energia dispunha dos meios técnicos e legais para evitar a confusão.

A Comissão de Proteção de Dados (DPC) irlandesa aplica uma coima de 530 milhões de euros à Tik Tok e suspende as transferências de dados para a China

A Comissão de Proteção de Dados (DPC) irlandesa aplicou uma coima de 530 milhões de euros à TikTok por realizar transferências internacionais de dados através de acesso remoto a partir da China sem aplicar as garantias adequadas exigidas pelo RGPD ou cumprir o seu dever de informar os utilizadores. Apesar de a notícia ter sido divulgada em maio de 2025, a [decisão](#) só foi publicada em outubro.

A DPC concluiu que a empresa demandada não avaliou adequadamente a legislação chinesa no âmbito do acesso remoto, com base na premissa errónea de que as autoridades chinesas não poderiam aceder legalmente a dados armazenados fora do país. Além disso, a empresa não demonstrou que leis como a Lei dos Serviços de Informações Nacionais, a Lei de Combate à Espionagem e a Lei de Segurança Cibernética não se aplicavam aos dados durante o seu tratamento na China.

A DPC examinou também as medidas complementares adotadas pela rede social para reforçar as suas cláusulas contratuais-tipo (CCT), incluindo medidas técnicas, contratuais e organizativas. Embora estas medidas fossem relevantes, foram consideradas insuficientes para compensar as deficiências legais da estrutura normativa chinesa, especialmente porque não foi realizada uma análise adequada da estrutura para determinar o nível inicial de risco.

No que respeita às exceções do artigo 49.º do RGPD, a DPC determinou que as mesmas não eram aplicáveis, uma vez que as transferências não eram ocasionais, mas sistemáticas e contínuas.

Por fim, no que diz respeito à transparência, a política de privacidade da rede social não mencionava a China como país de destino e não explicava a natureza do acesso remoto. Embora estas omissões tenham sido posteriormente corrigidas, a DPC considerou que o artigo 13.º, n.º 1, al. f) do RGPD tinha sido violado durante mais de dois anos.

Após a publicação desta resolução, a AEPD emitiu uma série de [recomendações](#) aos utilizadores, especialmente aos mais jovens, incentivando-os a que:

- Leiam atentamente as notificações e políticas de privacidade.
- Revejam as definições de privacidade e as permissões concedidas nas aplicações.
- Ponderem se desejam continuar a utilizar serviços que transferem dados para países sem garantias equivalentes às da Europa.
- Sejam prudentes ao partilhar informações sensíveis nas redes sociais.

Publicadas várias sanções a diversas farmácias catalãs por irregularidades no tratamento de dados pessoais

A AEPD publicou 18 resoluções sancionatórias contra várias farmácias catalãs por irregularidades no tratamento de dados pessoais de residentes em lares de idosos (uma delas pode ser consultada [neste link](#)), incluindo acesso não autorizado e transmissão de dados de saúde por meios inseguros.

As farmácias sancionadas preparavam os chamados "Sistemas de Dosagem Personalizada" (PDS) para os centros residenciais, que envolviam a gestão de categorias especiais de dados, como as normas clínicas dos doentes. No entanto, a transmissão desta informação foi realizada por correio eletrónico não encriptado, o que constitui uma grave violação de segurança. Embora as farmácias tenham alegado responsabilidade conjunta com os lares de idosos, a AEPD determinou que estas atuavam como responsáveis pelo tratamento dos dados.

Entre as infrações mais significativas, destacou-se a violação do artigo 6.º do RGPD, pela elaboração dos SPD sem o devido consentimento informado. A regulamentação do setor e o guia de SPD da Catalunha exigem uma autorização explícita e documentada, requisito que não foi cumprido. O artigo 14.º do RGPD, relativo ao dever de informar quando os dados são obtidos de terceiros, foi também violado, uma vez que os titulares dos dados não

receberam informações sobre a identidade do responsável pelo tratamento, as finalidades do tratamento, os seus direitos e outros elementos necessários. Embora algumas farmácias tenham exibido cartazes informativos, a natureza dos dados tratados e as circunstâncias dos doentes — residentes em lares de idosos — demonstram que esta informação não chegou efetivamente aos afetados.

Além disso, foi sancionada a violação do artigo 32.º do RGPD pela ausência de medidas técnicas e organizativas adequadas, como a encriptação na transmissão de mensagens de correio eletrónico. Algumas resoluções destacaram ainda o incumprimento do acordo obrigatório com a Administração e a Ordem dos Farmacêuticos da Catalunha, pré-requisito para a prestação do serviço de SPD. Esta omissão significava que o tratamento de dados de saúde não tinha base legal nos termos do artigo 9.º do RGPD, que regula o tratamento de categorias especiais de dados.

Indeferido o recurso interposto por uma empresa de telecomunicações para adiar a aplicação de medidas corretivas até à conclusão do processo judicial perante a Audiência Nacional

A AEPD [indeferiu](#) o recurso interposto por uma conhecida empresa de telecomunicações que opera em Espanha contra uma resolução que identificou duas infrações graves, sancionadas com uma coima substancial e a imposição de uma medida corretiva.

A AEPD suspendeu provisoriamente a execução da obrigação de pagamento das coimas quando a empresa anunciou a sua intenção de apresentar um recurso, mas negou a suspensão da medida corretiva porque prevaleceu o interesse geral na proteção de dados e a necessidade de evitar danos graves e irreparáveis aos titulares dos dados. A este respeito, a AEPD confirma na sua resolução que os procedimentos aplicados pela empresa sancionada para a emissão de cartões SIM duplicados permitiam, na prática, falhas e exceções que facilitavam o roubo de identidade.

A AEPD refere que o protocolo para a duplicação de cartões SIM priorizava as operações comerciais sem valorizar suficientemente o risco real e elevado de fraude e a necessidade de medidas técnicas e organizativas eficazes, violando, assim, o princípio da proteção de dados desde a conceção, previsto no artigo 25.º do RGPD. A resolução sublinha que a falta de controlos robustos pode causar danos graves e irreparáveis aos titulares dos dados e, por fim, embora confirme a suspensão cautelar do pagamento de coimas devido à existência de exigências legais, decide rejeitar a suspensão da medida corretiva por considerar que o interesse geral na proteção de dados de um número muito significativo de afetados deve prevalecer sobre o interesse económico da entidade, alinhando, assim, com a doutrina da Audiência Nacional que, em casos análogos, negou a suspensão das medidas de adequação ao RGPD por não gerarem efeitos irreversíveis e pelo facto de eventuais danos serem ressarcíveis.

O ICO aplica uma coima de 14 milhões de libras por graves falhas de segurança que expuseram os dados de 6,6 milhões de pessoas

O *Information Commissioner's Office* (ICO) do Reino Unido [aplicou](#) a uma empresa de consultoria e à sua subsidiária uma coima total de 14 milhões de libras por falhas de segurança ocorridas em 2023 que afetaram cerca de 6,6 milhões de pessoas. O incidente teve origem num ciberataque que permitiu o acesso não autorizado a informações pessoais e, em alguns casos, a dados sensíveis, incluindo registos de pensões, informações financeiras, dados de funcionários e antecedentes criminais.

A investigação do ICO identificou graves falhas de segurança, nomeadamente um atraso de 58 horas na resposta a um alerta crítico, face ao objetivo interno de uma hora. A investigação constatou ainda a falta de testes de intrusão regulares e de avaliações de risco atualizadas em sistemas que tratam milhões de registos pessoais.

A autoridade concluiu que estas deficiências constituíam violações dos artigos 5.º, n.º 1, al. f), 32.º, n.º 1 e 32.º, n.º 2 do UK RGPD

(Regulamento Geral de Proteção de Dados do Reino Unido), relativos ao princípio da integridade e confidencialidade dos dados e à obrigação de implementar medidas técnicas e organizativas adequadas.

O ICO enfatizou que a magnitude do incidente e a falta de controlos preventivos adequados demonstram negligência na gestão dos riscos cibernéticos, especialmente grave nas empresas que prestam serviços críticos de administração de pensões e gestão de dados financeiros.

Uma operadora foi sancionada por não verificar a identidade durante uma mudança de titularidade e duplicação de cartão SIM, facilitando a fraude com dados pessoais

A autoridade de proteção de dados sancionou uma [operadora de telecomunicações](#) por violar o artigo 6.º, n.º 1 do RGPD ao transferir a titularidade de uma linha móvel e emitir um cartão SIM duplicado sem o consentimento do titular e sem aplicar os controlos de verificação estabelecidos nos seus próprios protocolos. A resolução sublinha que a entidade, enquanto responsável pelo tratamento de dados, deve garantir a licitude do tratamento de dados pessoais, o que implica não só a implementação de medidas técnicas e organizativas, mas também a garantia da sua correta aplicação em cada caso.

A omissão da dupla verificação e a falha em comprovar a identidade do titular dos dados são consideradas como tendo permitido que um terceiro se fizesse passar pelo titular, acedendo a dados pessoais e possibilitando a fraude bancária. A AEPD rejeita os argumentos da operadora relativamente à existência de uma base legitimadora e à suficiência das suas medidas, afirmando que a responsabilidade não pode ser transferida para terceiros nem pode ser justificada por erros isolados de agentes ou fornecedores. A conduta é classificada como negligente, uma vez que a entidade não agiu com a diligência necessária no tratamento de dados pessoais.

A coima aplicada ascende a 300.000 euros, tendo em conta a gravidade da infração, os

danos causados e a ligação da atividade ao tratamento massivo de dados pessoais.

Declarada a existência de violação da segurança no tratamento de dados após o roubo de um equipamento informático com informações policiais sobre desaparecimentos e condenações, que não possuía palavra-passe

Em maio de 2022, ocorreu o roubo de um computador e de uma *pendrive* pertencentes a um investigador que colaborava com o Centro Nacional para Pessoas Desaparecidas, afeto à Direção-Geral de Coordenação e Estudos (DGCE). Ambos os dispositivos continham informações altamente sensíveis, incluindo relatórios policiais sobre desaparecimentos, dados de saúde e condenações criminais, assim como gravações de entrevistas com vítimas e os seus familiares. O computador não possuía palavra-passe de acesso, permitindo aceder diretamente ao seu conteúdo.

A DGCE defendeu que o tratamento deveria reger-se pela Lei Orgânica 7/2021, de 26 de maio, que transpõe a Diretiva (UE) 2016/680 e regula o tratamento efetuado pelas autoridades competentes para efeitos de prevenção ou deteção de infrações penais. No entanto, a Agência considerou que os dados foram utilizados para fins científicos e estatísticos — o desenvolvimento da ferramenta preditiva SERDESVI — e não no âmbito de uma investigação criminal específica, sendo, portanto, aplicável o RGPD.

A AEPD identificou graves deficiências estruturais nas medidas de segurança, incluindo a ausência de encriptação, palavras-passe, cópias de segurança e controlo de inventário. Além disso, rejeitou a alegação de que o incidente poderia ser considerado um “erro humano isolado”, uma vez que revelou uma falha sistémica na gestão da segurança do tratamento de dados e nos protocolos internos de notificação de violações.

Por conseguinte, a Agência declarou que ocorreu uma violação do artigo 32.º do RGPD, embora, de acordo com o artigo 83.º, n.º 7 do RGPD e o artigo 77.º, n.º 2 da Lei Orgânica 3/2018, relativa à Proteção de Dados Pessoais

e Garantia dos Direitos Digitais (LOPD-gdd), não tenha imposto uma sanção pecuniária por se tratar de uma entidade do setor público. O recurso gracioso interposto foi indeferido pela Agência, que manteve a sua decisão.

Empresa de aluguer de automóveis sancionada em 100.000 euros por negar alugueres a clientes que constavam da sua lista de exclusões

A AEPD aplicou uma coima de 100.000 euros (reduzida para 80.000 euros por pagamento voluntário) a uma empresa de aluguer de automóveis por incluir os dados de um cliente num sistema interno de alertas que o impedia de efetuar novas reservas, sem uma base legal válida para o efeito, nos termos do artigo 6.º, n.º 1 do RGPD.

O caso remonta a 2018, quando o reclamante, cliente da empresa, deixou as chaves do carro com um terceiro, tendo ocorrido o desaparecimento temporário do veículo. A empresa registou o incidente e associou os dados do cliente a um alerta interno, o que, três anos depois, levou à recusa de um novo aluguer. A entidade argumentou que o tratamento dos dados se baseava inicialmente na antiga Lei Orgânica 15/1999 e que, após a aplicação do RGPD, passou a basear-se no seu interesse legítimo, tendo realizado um teste de ponderação e uma avaliação de impacto.

A Agência rejeita estes argumentos e conclui que as condições gerais de contratação de 2018 não informavam os clientes da possibilidade de conservação de dados para os excluir de contratos futuros, pelo que o tratamento não poderia ser considerado necessário para a execução do contrato. Considera ainda que não existe um teste de ponderação válido de interesse legítimo ou de proporcionalidade, considerando excessiva a criação de listas de exclusão sem prova objetiva de fraude ou falta de pagamento.

A AEPD equipara o caso à inclusão indevida em “listas negras” ou ficheiros de mora, devido à falta das garantias necessárias, e declara uma violação do artigo 6.º, n.º 1, do RGPD, aplicando a referida sanção.

O acesso ao histórico clínico de um trabalhador para fins organizativos internos num centro de saúde constitui uma violação do princípio da integridade e confidencialidade

A AEPD [declarou](#) a existência de uma violação do artigo 5.º, n.º 1, al. f) do RGPD por violação do princípio da integridade e confidencialidade, emitindo uma admoestação à *Conselleria* de Saúde da Comunidade Valenciana e ordenando a adoção de medidas corretivas no prazo de três meses.

O processo teve início após uma queixa apresentada por um profissional de saúde que, durante uma situação de incapacidade temporária, detetou diversos acessos injustificados ao seu registo médico por parte de funcionários do centro de saúde onde trabalhava. Segundo a denúncia, os dados foram também referidos num grupo de WhatsApp do próprio centro.

Durante a tramitação do processo, a *Conselleria* solicitou a suspensão do processo devido à existência de um processo penal paralelo pela alegada descoberta e divulgação de segredos, invocando o princípio *non bis in idem*. A Agência rejeitou este pedido, referindo que os processos penais e administrativos podem coexistir quando protegem interesses jurídicos distintos.

Embora o processo criminal tenha sido concluído com uma decisão de arquivamento provisório, considerando que os acessos foram realizados por instruções do coordenador e não com a intenção de violar a privacidade do titular dos dados, a AEPD enfatizou que o direito à proteção de dados é mais amplo do que o direito à privacidade. A AEPD confirmou que os acessos foram efetuados para verificação da situação laboral do reclamante, finalidade que não se enquadra na exceção para fins clínicos prevista nos artigos 9.º, n.º 2, al. h) e 9.º, n.º 3 do RGPD, reservada ao tratamento de dados para efeitos médicos.

Consequentemente, a AEPD adverte a *Conselleria* e insta-a a implementar medidas técnicas e organizativas que garantam a confidencialidade dos registos médicos.

Uma empresa foi sancionada por uma violação de dados no seu diretório de utilizadores que permitiu a publicação de mais de 2600 números de telefone e alias

A AEPD [sancionou](#) a Bizum, S.L. após de ser notificada uma violação de dados pessoais que afetou 2634 utilizadores do serviço. A entidade sancionada detetou em novembro de 2023 que um site público continha números de telemóvel e alias (nomes abreviados) extraídos do seu "Diretório Bizum", uma base de dados que associa cada número à identidade do utilizador.

A investigação interna revelou que este acesso não autorizado ocorreu mais de um ano antes, em setembro de 2022, quando um utilizador legítimo de uma instituição bancária, membro do sistema "Bizum", fez mais de 20.000 consultas automáticas e sequenciais ao serviço de validação de utilizador, o que permitiu a recolha de alias associadas a vários números de telefone. Embora a Bizum tenha bloqueado o utilizador responsável no mesmo dia, após detetar um volume invulgarmente elevado de consultas, inicialmente não identificou que tivesse ocorrido uma violação de dados. A publicação subsequente de alguns destes registos online obrigou a empresa a reportar formalmente o incidente e a remover as informações expostas do site afetado.

O RGPD exige a adoção de medidas técnicas e organizativas adequadas para garantir a segurança dos dados pessoais e impedir o acesso não autorizado. A AEPD considerou que a Bizum violou o artigo 32.º do RGPD por não limitar ou controlar suficientemente o acesso ao "Diretório Bizum" e por não avaliar adequadamente os riscos associados à função de pesquisa de alias. Além disso, a falta de mecanismos de monitorização eficazes permitiu que a violação passasse despercebida durante mais de um ano, evidenciando deficiências na deteção precoce e na resposta a incidentes de segurança. A infração foi classificada como grave, nos termos do Artigo 73.º, alínea f) da LOPD-gdd, relativo à falta de medidas de segurança adequadas exigidas pelo Artigo 32.º, n.º 1 do RGPD, cabendo à Bizum provar que implementou um nível de proteção adequado ao risco, o que não conseguiu fazer.

A infração é punível com coima de 100.000 euros, valor determinado com base no volume de negócios e nos critérios de proporcionalidade e efeito dissuasor. Além disso, a AEPD aplicou uma medida corretiva: a Bizum deve demonstrar, no prazo máximo de seis meses, a implementação de mecanismos de segurança reforçados no seu diretório, garantindo que os alias só podem ser acedidos quando for estritamente necessário para a transação e impedindo qualquer possibilidade de consultas automatizadas ou em massa não autorizadas. Estes requisitos visam prevenir a recorrência de incidentes e elevar o nível de proteção do utilizador para além da sanção pecuniária.

Coima de 150.000 euros por contratação online fraudulenta de serviços de comunicações eletrónicas

A [resolução](#) analisa um caso de contratação fraudulenta de uma linha de telemóvel em nome de uma pessoa que negou qualquer vínculo com a entidade sancionada. A AEPD concluiu que o tratamento de dados pessoais carecia de fundamento jurídico, violando o artigo 6.º, n.º 1 do RGPD, e, consequentemente, aplicou uma coima de 150.000 euros. A investigação apurou que o processo de registo online permitido pela operadora apenas verificava a estrutura do documento de identidade nacional (DNI), baseava-se na assinatura de um PIN enviado por SMS para um número fornecido pelo requerente através de um prestador de serviços fidedigno e adia a verificação visual do DNI até à fase de entrega do cartão SIM por correio, sem prova suficiente da sua efetiva realização. A Agência considera que estas medidas não garantem a identificação do verdadeiro titular dos dados nem a licitude do tratamento, e que o contrato só se formaliza efetivamente quando, sendo o caso, a verificação ocorre aquando da entrega.

A resolução enfatiza a responsabilidade proativa do responsável pelo tratamento (artigos 5.º, n.º 2, 24.º e 25.º do RGPD) e a necessidade de adotar medidas técnicas e organizativas adequadas ao risco (artigos 25.º e 32.º do RGPD) para prevenir o roubo de identidade. Reitera a doutrina da Audiência Nacional e do Supremo Tribunal, segundo a qual a intervenção fraudulenta de terceiros não

exclui a infração se não tiver sido exercida a diligência exigível na verificação da identidade. Para efeitos de graduação, considera-se a natureza e a gravidade da infração, a negligência observada, o tratamento de dados de identificação — com especial referência ao Documento Nacional de Identidade (DNI), dado particularmente sensível devido ao seu potencial de dano —, o grau de responsabilidade pelas deficiências na conceção dos controlos, a ligação da atividade ao tratamento de dados e as sanções anteriores. As circunstâncias atenuantes invocadas (remediação subsequente, cooperação, falta de benefício e não tratamento de categorias especiais) são rejeitadas, uma vez que não eliminam a necessidade de uma sanção eficaz, proporcional e dissuasora. Assim sendo, mantém-se a infração ao Artigo 6.º, n.º 1 do RGPD e a coima acima referida.

Sanção pela disseminação de imagens manipuladas com ferramentas de inteligência artificial

O procedimento sancionatório foi iniciado após uma série de notícias publicadas nos meios de comunicação social e o registo de uma reclamação individual. A investigação preliminar confirmou a difusão de imagens manipuladas com ferramentas de inteligência artificial que associavam rostos reais a corpos nus através de serviços de mensagens e plataformas online.

A [resolução](#) da AEPD refere que tal difusão constitui o tratamento de dados pessoais sem base legítima, nos termos do Artigo 6.º, n.º 1 do RGPD, e designa o seu autor como responsável pelo tratamento de dados (Artigo 4.º, n.º 7 do RGPD), ao determinar as finalidades e os meios da difusão. É reiterada a doutrina relativa ao poder de disposição do titular relativamente à sua imagem e a proteção reforçada especial concedida aos menores (Artigo 84.º da LOPD-gdd).

Para efeitos sancionatórios, a infração enquadra-se no Artigo 83.º, n.º 5, do RGPD (princípios básicos e condições de licitude), com proposta inicial de uma coima de 2000 €, tendo em conta a natureza dos factos, o seu âmbito e o impacto nos direitos fundamentais. Durante o processo, o alegado infrator invocou o Artigo 85.º da Lei 39/2015, de 1 de outubro,

sobre o Procedimento Administrativo Comum das Administrações Públicas (LPACAP), reconhecendo a responsabilidade e efetuando um pagamento voluntário, pelo que foram aplicadas duas reduções cumulativas de 20% cada, reduzindo a coima para 1200 euros. A AEPD declarou a prática da infração, confirmou a sanção daí resultante e aceitou encerrar o processo, condicionando as reduções à desistência de eventuais recursos interpostos pela via administrativa.

A resolução enfatiza a ilicitude da divulgação não consentida de imagens (incluindo a sua manipulação sintética) e a necessidade de prevenir esse tratamento, alertando que, caso se confirmem incidentes semelhantes, poderão ser impostas medidas corretivas adicionais (Art. 58.º, n.º 2 do RGPD) para garantir a cessação da conduta e a proteção adequada dos afetados.

A AEPD sanciona um subcontratante para o tratamento pela subcontratação em cadeia não autorizada pelo responsável

Na sua decisão sobre este procedimento sancionatório, a AEPD [aborda](#) o regime de responsabilidade nas cadeias de subcontratação e os requisitos formais para os contratos de subcontratante para o tratamento.

Os factos começaram quando uma cliente, para se registar como titular conjunta de uma conta bancária, enviou documentos sensíveis, incluindo uma cópia do seu documento de identidade nacional (DNI), através de um serviço de entrega expresso. A cadeia de tratamento envolvia uma empresa inicial que atuava como subcontratante para o tratamento de dados do banco, uma empresa de entregas expresso que atuava como subcontratante ulterior do banco e uma terceira empresa que atuava como subcontratante ulterior da empresa de entregas expresso. No entanto, os documentos nunca chegaram ao destinatário final.

A investigação da AEPD revelou que a entidade bancária, na qualidade de responsável pelo tratamento, apenas tinha aprovado a subcontratação de serviços da primeira empresa subcontratante a um fornecedor diferente da empresa de entregas e da terceira empresa. Assim sendo, nem a primeira

empresa subcontratante nem a empresa de entregas possuíam a autorização prévia e expressa do responsável pelo tratamento para utilizar estes subcontratantes ulteriores adicionais.

A AEPD aplicou duas coimas de 40.000 euros cada uma. A primeira, por infração ao artigo 28.º, n.º 2 do RGPD, pelo facto de a empresa de entregas ter recorrido a subcontratantes ulteriores sem a devida autorização do responsável pelo tratamento. A segunda, por infração ao artigo 28.º, n.º 4, dado que o contrato de tratamento de dados não continha alguns dos elementos essenciais exigidos pelo artigo 28.º: não identificava o responsável pelo tratamento dos dados, não continha uma descrição detalhada do tratamento, omitia a obrigação de agir exclusivamente mediante instruções documentadas do responsável pelo tratamento e as medidas de segurança eram descritas de forma genérica e insuficiente.

A resolução sublinha que a complexidade operacional das cadeias de subcontratação não justifica o incumprimento regulamentar, recordando que o RGPD exige a identificação do responsável pelo tratamento em cada nível da subcontratação.

Instituição financeira sancionada por violação de segurança que expôs dados de milhões de clientes

Em novembro de 2023, uma instituição de crédito foi vítima de um ciberataque de negação de serviço (DDoS), que resultou no acesso não autorizado a dados pessoais como o nome, o número de identidade nacional, a morada fiscal e a data de nascimento. Estes dados eram tratados pela instituição quer como responsável pelo tratamento dos seus próprios clientes quer como subcontratante para o tratamentos de dados para outras entidades financeiras e seguradoras. O incidente afetou aproximadamente dois milhões de pessoas, comprometendo informações sensíveis como o nome, o número de identidade nacional, a morada fiscal e a data de nascimento.

Após a sua investigação, a AEPD concluiu na [resolução](#) que as medidas técnicas e organizativas implementadas pela instituição foram inadequadas para garantir a integridade e a confidencialidade dos dados pessoais.

Além disso, a resolução sublinha que a instituição financeira não só deixou de implementar as medidas de segurança adequadas, como também prolongou a duração da violação, o que aumentou o risco de utilização indevida e fraude.

Deste modo, considerou-se que o princípio da integridade e confidencialidade, tal como estabelecido no artigo 5.º, n.º 1, al. f) do RGPD, foi violado, tendo sido aplicada uma coima de 10.000 euros, sem avaliar se as medidas de segurança estavam em conformidade com os requisitos do artigo 32.º do RGPD.

Foi imposta uma coima a um condomínio residencial por captar imagens dos seus moradores durante a recolha de encomendas

A AEPD [sancionou](#) uma sociedade civil privada que tinha implementado um sistema de recolha de encomendas para os residentes que utilizava a captação de uma fotografia para identificar quem recebia as encomendas. A fotografia era armazenada num computador, e os moradores não tinham sido informados sobre este tratamento dos seus dados.

A arguida, enquanto responsável pelo tratamento de dados, tratava as imagens dos residentes apesar de tal não ser necessário para o fim pretendido. A AEPD não aceita os argumentos de que o tratamento se limitou ao momento específico da entrega e indica que não há registo de qualquer avaliação realizada relativamente aos direitos, liberdades e interesses dos titulares dos dados, tendo sido feita apenas referência às necessidades organizativas do condomínio gerido pela empresa.

Pelo exposto, a AEPD determina que o princípio da minimização dos dados, previsto no artigo 5.º, n.º 1, alínea c), do RGPD, foi violado e aplica uma coima de 2000 euros à arguida.

A AEPD elogia a rápida correção do incumprimento da legislação de proteção de dados

A reclamada tinha implementado um sistema de controlo de ponto constituído por um tablet

que funcionava como uma câmara de gravação de imagens, permanentemente ativa, e um teclado alfanumérico virtual junto ao ecrã. O sistema operava utilizando o número completo do documento de identidade nacional do trabalhador ou descarregando um código QR para o seu dispositivo móvel e colocando-o em frente ao ecrã do tablet.

A empresa descobriu que a aplicação estava configurada incorretamente para capturar imagens no momento do registo de entrada e saída. Assim, solicitou que o fornecedor da aplicação desativasse esta opção, pois tirar fotografias não era necessário para gerir os registos de ponto e não estava a ocorrer qualquer tratamento de dados.

A AEPD [valorizou](#) a pronta resposta da empresa na correção da configuração errónea, concluindo que não houve intenção de utilizar os dados de forma desproporcional, mas sim um erro técnico que foi retificado logo que detetado. Além disso, não existiam provas de que a entidade responsável tivesse acedido às fotografias tiradas ou de que estas tivessem sido utilizadas para qualquer finalidade.

Por todos os motivos acima expostos, a AEPD decidiu não impor qualquer sanção por incumprimento das normas de proteção de dados.

Uma clínica de estética criou um grupo no WhatsApp com vários dos seus clientes sem o seu consentimento para promover os seus serviços

A AEPD [sancionou](#) uma clínica de estética em 30.000 euros por violação do princípio da integridade e confidencialidade reconhecido no artigo 5.º, n.º 1, al. f) do RGPD. A clínica criou um grupo no WhatsApp para promover os seus serviços, incluindo vários clientes sem o seu consentimento e tornando visíveis os seus números de telefone. Esta ação, dada a própria natureza do serviço prestado pela clínica, revelou indiretamente os dados de saúde dos participantes. Em resposta às queixas, a clínica abandonou o grupo sem o fechar de imediato, permitindo que a informação permanecesse exposta.

Além da coima, a AEPD ordenou que a clínica demonstrasse, no prazo de um mês, a

eliminação do grupo do WhatsApp e, no prazo de três meses, a implementação de sistemas de comunicação que garantam a confidencialidade dos membros, de forma a que apenas o administrador possa ver os membros do grupo.

A AEPD declarou que a inclusão de informação no exterior de um envelope com avisos como "diligência de apreensão" ou "notificação de ordem de execução" viola o princípio da confidencialidade

A AEPD iniciou um processo sancionatório contra uma Câmara Municipal por uma possível violação do princípio da confidencialidade, consagrado no artigo 5.º, n.º 1, al. f) do RGPD, após uma denúncia. O Departamento de Receitas da Câmara Municipal enviou duas notificações por correio registado ao denunciante. Os envelopes exibiam visivelmente, respetivamente, as palavras "diligência de apreensão" e "notificação de ordem de execução", ambas seguidas de um número de referência.

Embora a Câmara Municipal tenha corrigido esta prática durante o processo, substituindo as palavras acima referidas por "notificação administrativa", a AEPD [confirmou](#) a infração ao artigo 5.º, n.º 1, al. f) do RGPD. A AEPD considerou que a redação inicial permitia a terceiros tomar conhecimento da situação fiscal do denunciante. Como a Câmara Municipal demonstrou ter adotado medidas corretivas, a

aplicação de uma coima não foi considerada necessária.

Sanção por violação do princípio da proteção de dados desde a conceção e por defeito

O Instituto Nacional de Cibersegurança de Espanha (INCIBE) organizou um curso online massivo (MOOC) cuja plataforma, devido a um erro de configuração, permitiu que determinados dados pessoais dos participantes, incluindo nomes, apelidos, endereços de e-mail, cidade e país, ficassem visíveis para outros utilizadores sem consentimento ou informação adequada, o que foi comunicado à AEPD.

A AEPD instaurou um processo por alegada violação do artigo 25.º do RGPD (proteção de dados desde a conceção e por defeito) e do artigo 5.º, n.º 1, al. f) do RGPD (integridade e confidencialidade dos dados). A análise dos factos apurados confirmou que a configuração por defeito da plataforma permitia a difusão não autorizada de dados pessoais entre os utilizadores e que as medidas técnicas e organizativas necessárias para proteger esses dados não foram implementadas adequadamente.

A [resolução](#) arquiva o processo por alegada violação do artigo 5.º, n.º 1, alínea f), do RGPD, mas considera que o princípio da privacidade desde a conceção e por defeito foi violado e, após avaliar os argumentos e a conduta da entidade, impõe uma sanção de 2000 euros.

Acórdãos

Meta condenada a pagar mais de 500 milhões de euros por concorrência desleal devido a violação do RGPD

O [acórdão](#) do Tribunal Comercial n.º 15 de Madrid, datado de 19 de novembro de 2025, resolve uma ação interposta por 87 editoras de imprensa, agências de notícias e estações de rádio espanholas contra a Meta Platforms Ireland Limited por concorrência desleal decorrente de violações em matéria de proteção de dados. O período analisado abrange desde 25 de maio de 2018 (entrada em vigor do RGPD) até 31 de julho de 2023.

O tribunal determinou que a Meta violou o RGPD nos seus serviços Facebook e Instagram ao realizar publicidade comportamental (publicidade baseada na observação contínua do comportamento do utilizador para criar perfis específicos e exibir anúncios personalizados). As principais infrações detetadas são:

1. Infração do artigo 6.º, n.º 1, al. b) do RGPD (fundamento jurídico para a execução contratual): A Meta utilizou indevidamente o fundamento jurídico de "necessidade para a execução do contrato" para justificar o tratamento de dados para fins publicitários, quando tal publicidade não era necessária nem essencial para a prestação do serviço de rede social. O Comité Europeu para a Proteção de Dados (CEPD) concluiu que a Meta não tinha o direito de invocar este fundamento jurídico para o tratamento de dados para fins de publicidade comportamental.
2. Infração do artigo 6.º, n.º 1, al. f) do RGPD (interesse legítimo): entre abril e julho de 2023, a Meta alterou o seu fundamento

jurídico para "interesse legítimo", tornando o tratamento igualmente ilícito, uma vez que não cumpria a necessária ponderação de interesses.

3. Infração do princípio da transparência (artigos 5.º, n.º 1 al. a), 12.º, n.º 1 e 13.º, n.º 1, al. c) do RGPD): A Meta não informou claramente os utilizadores sobre as finalidades do tratamento nem sobre o fundamento jurídico utilizado.
4. Violação do princípio da equidade (Artigo 5.º, n.º 1, al. a) do RGPD): foi criada uma assimetria de informação que colocava os utilizadores numa desvantagem sistemática, limitando o seu controlo sobre os seus dados pessoais através de uma política de "aceitar ou rejeitar".
5. Violação do princípio da minimização de dados (artigo 5.º, n.º 1, al. c) do RGPD): A Meta recolheu dados de forma generalizada e indiscriminada, incluindo potencialmente categorias especiais de dados (artigo 9.º, n.º 1 do RGPD) sem consentimento explícito.

Foi determinado que a Meta obteve uma vantagem competitiva significativa no mercado da publicidade online ao tratar ilegalmente dados de utilizadores do Instagram e do Facebook para publicidade personalizada, infringindo as normas de proteção de dados. Esta vantagem não pôde ser igualada pelos seus concorrentes, os meios de comunicação que apresentaram a queixa.

O tribunal julgou parcialmente procedente a queixa e condenou a Meta ao pagamento de uma indemnização por concorrência desleal, nos termos do artigo 15.º, n.º 1 da Lei da Concorrência Desleal, no valor total de 542.170.719,69 euros.

Conclusões do TJUE sobre a necessidade (ou não) de autorização judicial prévia apreender e-mails em inspeções de concorrência

O Tribunal de Justiça da União Europeia publicou as [conclusões da advogada-geral Medina](#) sobre as apreensões de e-mails empresariais por parte das autoridades nacionais da concorrência. De acordo com estas conclusões, o direito fundamental à proteção de dados pessoais não exige uma autorização judicial prévia para que uma autoridade da concorrência aceda a e-mails profissionais no âmbito de uma investigação. Este acesso é considerado compatível com o direito da UE porque a sua finalidade é estritamente empresarial, visando a deteção de práticas anticoncorrenciais, e afeta as pessoas singulares apenas de forma incidental.

O caso teve origem em Portugal, onde a autoridade nacional da concorrência apreendeu e-mails trocados entre funcionários de várias empresas sob investigação. Estas empresas argumentaram que a ação violava o seu direito à privacidade da correspondência e que a apreensão exigia a autorização de um juiz de instrução, e não apenas do Ministério Público. O tribunal português remeteu o caso para o Tribunal de Justiça, questionando se o facto de os e-mails serem trocados entre particulares, mesmo que utilizassem endereços profissionais, exigia um nível de proteção mais elevado, comparável ao concedido à correspondência privada. Posteriormente, a Grande Secção do Tribunal solicitou novas conclusões, em particular após o [acórdão Bezirkshauptmannschaft Landeck](#), que estabeleceu critérios mais rigorosos para o acesso das autoridades a dados altamente sensíveis contidos num telemóvel.

A advogada-geral sublinha que esta jurisprudência não pode ser extrapolada, uma vez que os telemóveis podem conter informações pessoais detalhadas sobre múltiplos aspetos da vida privada, enquanto os e-mails empresariais se limitam a conteúdos profissionais e não permitem a reconstrução da esfera privada de um indivíduo. Por conseguinte, não é necessário um nível mais elevado de proteção ou um controlo judicial prévio obrigatório. Contudo, indica que o acesso a e-mails numa investigação da

concorrência constitui uma interferência na proteção de dados que só será legítima se forem adotadas garantias adequadas, como o respeito pelo princípio da proporcionalidade, o cumprimento das obrigações do RGPD, a existência de procedimentos formalizados e o controlo judicial posterior das atividades de inspeção.

A intervenção judicial prévia só seria necessária quando a apreensão ocorresse numa residência privada ou se destinasse a acusar criminalmente uma pessoa singular. Lembra ainda que os Estados-Membros podem optar por exigir mecanismos de autorização prévia — incluindo os emitidos pelo Ministério Público — se desejarem reforçar as garantias na sua legislação nacional.

A advogada-geral recomenda que as empresas sujeitas a investigações da concorrência revejam os seus protocolos de gestão e acesso a e-mails empresariais, formem os seus colaboradores sobre as obrigações aplicáveis e documentem adequadamente a informação a que as autoridades acederam, garantindo o respeito pela minimização e limitação da utilização de dados. Entretanto, o Tribunal de Justiça prossegue a sua deliberação, uma vez que as conclusões não são vinculativas e o acórdão final será proferido posteriormente.

O TJUE nega a isenção de responsabilidade às plataformas que divulguem dados pessoais e considera-as responsáveis pelo tratamento

A Russmedia Digital SRL, uma empresa romena, operava um mercado online onde os utilizadores publicavam anúncios, alguns dos quais continham dados pessoais e dados sensíveis de terceiros. O litígio originou uma decisão preliminar sobre se o operador da plataforma poderia beneficiar da isenção de responsabilidade concedida aos prestadores de serviços de alojamento ou se deveria ser considerado responsável pelo tratamento nos termos do RGPD.

O Tribunal de Justiça da União Europeia (TJUE) [declara](#) que o operador de um mercado online que publica anúncios gerados pelos utilizadores não pode ser considerado um mero intermediário neutro quando torna acessíveis

dados pessoais de terceiros e obtém um benefício comercial com essa divulgação.

O Tribunal concluiu que a empresa não se limitou a alojar passivamente o conteúdo, mas antes determinou as finalidades e os meios do tratamento ao organizar um mercado online com regras próprias, influenciando decisivamente a divulgação de dados pessoais. Deste modo, atua como responsável pelo tratamento (ou responsável conjunto) nos termos do RGPD. Consequentemente, o TJUE estabelece que estas plataformas não podem invocar a isenção de responsabilidade prevista na Diretiva 2000/31/CE (e-Commerce) para contornar as obrigações do RGPD.

A decisão impõe aos operadores a obrigação de identificar, antes da publicação, os anúncios que contenham dados sensíveis, verificar a legitimidade do anunciante e recusar a publicação caso não exista consentimento explícito ou outra exceção ao abrigo do artigo 9.º do RGPD, além de implementar medidas técnicas e organizativas para impedir a cópia e redistribuição ilícitas desses dados.

Acórdão da Audiência Nacional sobre a violação do artigo 6.º do RGPD em atividades de videovigilância com gravação de voz

A Audiência Nacional decidiu e proferiu um [recurso contencioso-administrativo](#) interposto da decisão da AEPD, de 23 de agosto de 2022, que aplicou uma coima de 6000 euros por violação do artigo 6.º do RGPD no âmbito de um sistema de videovigilância instalado num estabelecimento comercial aberto ao público. O litígio teve origem na gravação não só de imagens, mas também de som, especificamente de uma conversa entre uma funcionária e uma cliente, posteriormente mencionada na carta de despedimento. As provas incluem a entrega de documentação informativa geral sobre as câmaras e um "manual de videovigilância", bem como a admissão por parte do responsável de que o sistema possuía capacidades de gravação de áudio.

O Secção parte da premissa de que a imagem e a voz constituem dados pessoais e procede a uma ponderação entre os poderes de controlo do empregador, nos termos do artigo 20.º, n.º

3, do Real Decreto Legislativo 2/2015, de 23 de outubro, que aprova o texto consolidado da Lei do Estatuto dos Trabalhadores, e os direitos fundamentais do trabalhador, em conformidade com o artigo 89.º da LOPD-gdd e a jurisprudência do Tribunal Constitucional (entre outros, o Acórdão n.º 119/2022 e o Acórdão n.º 98/2000). Nesta ponderação, distingue entre a captação de imagens — que pode ser adequada e necessária em termos de segurança e monitorização, desde que se cumpram o dever de informação prévia e o princípio da proporcionalidade — e a gravação de voz — que é substancialmente mais intrusiva e exige uma justificação mais robusta, baseada nos riscos de segurança relevantes e respeitando os princípios da intervenção mínima e da proporcionalidade.

Aplicando este padrão, o Tribunal conclui que, embora tenha sido fornecida informação prévia sobre a existência de câmaras, a ativação da gravação áudio não foi comunicada de forma clara, expressa e específica, nem foi demonstrado que a gravação era necessária e proporcional para efeitos de controlo no local de trabalho. A gravação de conversas permite o acesso a conteúdos íntimos ou irrelevantes para o controlo do desempenho, existindo meios menos invasivos para os fins pretendidos. Consequentemente, o tratamento da gravação áudio carecia de uma base jurídica lícita suficiente, violando assim o artigo 6.º do RGPD.

Novos esclarecimentos do TJUE sobre a interpretação da Directiva “ePrivacy” relativamente ao envio de comunicações comerciais por correio eletrónico

Este [acórdão](#) aborda a relação entre a Diretiva *ePrivacy* e o RGPD no contexto das comunicações comerciais. O litígio decorre de uma sanção imposta pela autoridade de proteção de dados romena (ANSPDCP) a uma editora romena por violação dos artigos 5.º, 6.º, n.º 1, e 7.º do RGPD. A editora enviava uma newsletter por e-mail a utilizadores com contas gratuitas para incentivar subscrições pagas e argumentou que não necessitava de consentimento ao abrigo do artigo 13.º, n.º 2, da Diretiva *ePrivacy* (a exceção para clientes existentes).

O Tribunal de Justiça da União Europeia esclarece três pontos-chave relativos à aplicação da Diretiva *ePrivacy*: (i) uma newsletter com conteúdos informativos que incentive o consumo de conteúdos pagos constitui uma comunicação de venda direta na aceção do artigo 13.º, n.º 1, da Diretiva *ePrivacy*; (ii) a obtenção de um endereço de correio eletrónico através da criação de uma conta gratuita, que neste caso está também ligada a uma oferta de subscrição paga e a uma newsletter que promove o acesso premium, pode ser considerada como tendo sido conseguida no contexto de uma "venda", uma vez que constitui uma contraprestação indireta; e (iii) no caso de comunicações efetuadas no âmbito do artigo 13.º, n.º 2, da Diretiva *ePrivacy* (regra especial), a licitude do tratamento é regulada por esta norma especial, sem necessidade de um fundamento jurídico do artigo 6.º do RGPD (norma geral).

O TJUE pronuncia-se sobre os limites da recolha e conservação de dados biométricos e genéticos pela polícia

O TJUE decidiu uma questão prejudicial apresentada por um tribunal checo relativamente à recolha e conservação, pela polícia, de impressões digitais, fotografias e perfis de ADN em processos penais por infrações penais dolosas. O tribunal remetente questionava a compatibilidade da legislação checa com a Diretiva 2016/680 em três planos: (i) se os dados biométricos/ADN podem ser recolhidos indiscriminadamente de qualquer pessoa suspeita ou acusada de uma infração penal dolosa, tendo em conta o princípio da minimização de dados (artigo 4.º, n.º 1, al. c), do RGPD) e a estrita necessidade de dados relativos a condenações e infrações penais (artigo 10.º do RGPD); (ii) se esses dados podem ser conservados indefinidamente; e (iii) o que abrange o "Direito do Estado-Membro" (artigos 8.º e 10.º do RGPD) como base jurídica: apenas disposições gerais ou também jurisprudência nacional?

A decisão do [acórdão](#) indica que:

- "Direito dos Estados-Membros" compreende disposições de alcance geral que estabelecem os requisitos mínimos para a recolha, a conservação e o apagamento, tal como interpretados pela

jurisprudência nacional, desde que essa jurisprudência seja acessível e previsível, podendo, portanto, ser utilizada como fundamento jurídico para o tratamento.

- O direito da União não impede disposições que permitam a recolha de dados biométricos ou de ADN de suspeitos ou acusados de infrações penais dolosas, desde que (i) as finalidades específicas e concretas do tratamento não exijam a distinção entre as duas categorias, e (ii) as autoridades apliquem todos os princípios (minimização) e o teste da estrita necessidade, avaliando o caso concreto (gravidade e natureza da infração penal, circunstâncias, ligações a outros processos, antecedentes e perfil).
- É admitido que não exista um limite absoluto para o período de conservação destes dados se a lei estabelecer períodos adequados para revisão periódica e, em cada revisão, se verificar a estrita necessidade de continuar a conservar os dados. As normas internas da polícia podem servir de guia, mas não substituem em juízo a obrigação de justificar o cumprimento do teste da estrita necessidade.

O TJUE exige a notificação imediata dos passageiros sobre a utilização de câmaras corporais e o tratamento dos seus dados pessoais.

O Tribunal de Justiça da União Europeia interpreta o RGPD em relação à [utilização de câmaras corporais](#) por parte dos inspetores nos transportes públicos, estabelecendo que os dados pessoais obtidos através de gravação se consideram recolhidos diretamente do titular dos dados, mesmo que este não tome qualquer medida consciente para os fornecer. Por conseguinte, o responsável pelo tratamento de dados deve fornecer imediatamente ao titular dos dados determinadas informações essenciais, de acordo com o artigo 13.º do RGPD. Estas informações incluem a identidade e os dados de contacto do responsável pelo tratamento, as finalidades e a base jurídica do tratamento, os destinatários, o período de conservação e os direitos de acesso e apagamento.

O Tribunal esclarece que a recolha indireta de dados ocorre apenas quando o responsável pelo tratamento não tem contacto direto com o titular dos dados e obtém os dados de outra fonte. Nos casos de recolha direta, a obrigação de informar pode ser cumprida através de uma abordagem multinível: as informações mais relevantes podem ser indicadas num aviso visível, enquanto as restantes devem estar

disponíveis de forma completa e acessíveis noutra local.

O acórdão sublinha a importância da transparência e da proteção dos direitos dos titulares no tratamento de dados pessoais por videovigilância, exigindo que a informação seja prestada de forma clara e eficaz.

Contacte os nossos profissionais

Alejandro Padín

Sócio - Madrid

alejandro.padin@garrigues.com

Adrián León

Associado sénior - Alicante

adrian.leon@garrigues.com

Carina Casadesús

Associada - Barcelona

carina.casadesus@garrigues.com

Ignacio Suárez

Associado - Madrid

ignacio.suarez@garrigues.com

Laia Llambrich

Associada - Bilbao

laia.llambrich@garrigues.com

Sebastián Hassi

Associado principal - Santiago do Chile

sebastian.hassi@garrigues.com

Antonio Durán

Associado - Málaga

antonio.duran@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

Siga-nos em:



info@garrigues.com

garrigues.com

Esta publicação contém informações de carácter geral, que não constituem uma opinião profissional ou aconselhamento jurídico

© J&A Garrigues, S.L.P., todos os direitos reservados. É proibida a exploração, reprodução, distribuição, comunicação pública e transformação, total ou parcial, desta obra, sem a autorização escrita da J&A Garrigues, S.L.P.