GARRIGUES

Newsletter Economia de Dados, Privacidade e Cibersegurança

Novembro de 2025

Índice

1. **Os dados pessoais pseudonimizados são dados pessoais? Pontos-chave após o acórdão do Tribunal de Justiça da UE no caso EDPS contra SRB**

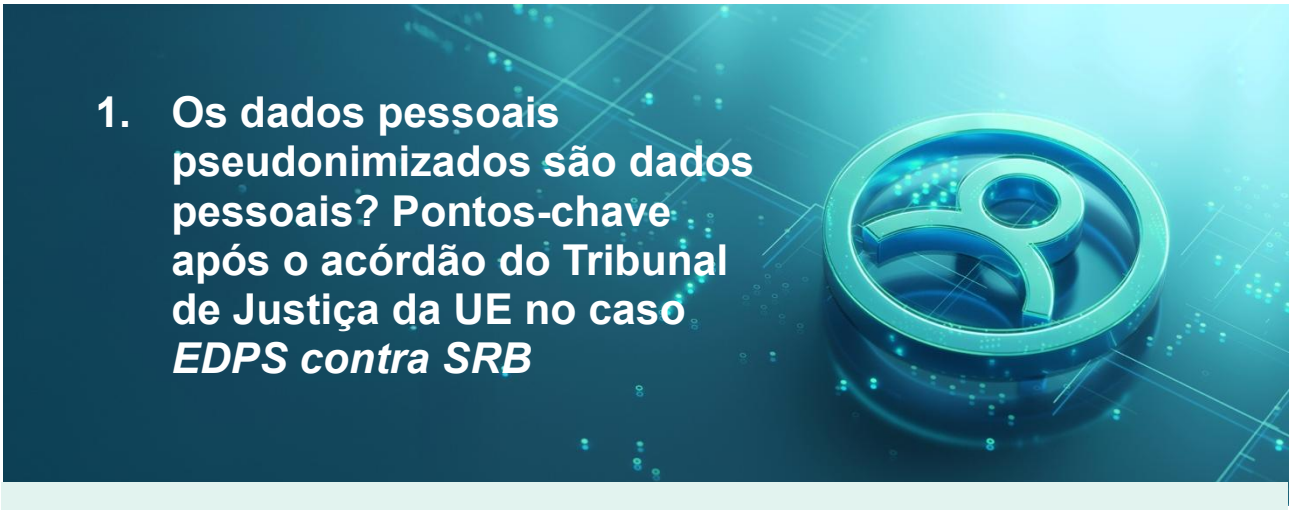
2. **Comparação da transposição da NIS II por parte de Portugal com a prevista em Espanha**

3. **Resoluções das autoridades de proteção de dados**

4. **Acórdãos**

5. **Atualidade**

1. Os dados pessoais pseudonimizados são dados pessoais? Pontos-chave após o acórdão do Tribunal de Justiça da UE no caso *EDPS contra SRB*



O acórdão do Tribunal de Justiça da União Europeia (TJUE) do passado dia 4 de setembro de 2025 no caso EDPS v SRB (processo C 413/23 P) constitui um marco importante na área da proteção de dados pessoais, por tratar um tema tão essencial para a prática como o próprio conceito de "dados pessoais".

Ignacio Suárez

Neste processo foram partes a Autoridade Europeia para a Proteção de Dados (AEPD ou *EDPS*, na sigla em inglês) e o Conselho Único de Resolução (CUR ou *SRB*, na sigla em inglês). O litígio decorre da resolução do Banco Popular (que ocorreu através de decisões do SRB (Conselho Único de Resolução) e do FROB em Espanha de 7 de junho de 2017) e do procedimento de "direito de audiência" iniciado pelo SRB em 2018 para avaliar a possível compensação para acionistas e credores, em que foram recolhidos dados e comentários através de um registo e um formulário online. Os comentários sobre a "avaliação 3" (1.104 no total) foram transmitidos a 17 de junho de 2019 pelo SRB à Deloitte através de um servidor virtual seguro. Após várias reclamações, a AEPD determinou, em 2020, que o SRB não tinha informado os titulares dos dados de que a Deloitte poderia ser destinatária dos seus dados na declaração de confidencialidade do processo. Esta decisão (posteriormente revista) foi contestada pelo SRB, levando à decisão do TJUE (Tribunal de Justiça da União Europeia) de 4 de setembro de 2025.

A questão mais significativa discutida neste caso, e que gerou um debate intenso e interessante entre os profissionais do setor, é se os dados pseudónimos ou pseudonimizados são inerentemente dados pessoais por defeito (uma vez que não são total e irrevogavelmente anonimizados), ou se podem ser considerados dados "não pessoais" para alguém que não consegue, sem um esforço desproporcional, ligar esses dados a uma pessoa singular.

Poder-se-ia pensar que algo tão básico não deveria estar em debate neste momento, mas a redação da legislação deu origem a diferentes perspetivas sobre o que deve, ou não, ser considerado um dado pessoal. Assim, surgiram duas visões diferentes sobre este conceito:

- **A doutrina absoluta**: que considera como dado pessoal qualquer informação que, direta ou indiretamente, possa ser associada a uma pessoa singular, por mais remota ou improvável que seja essa ligação.

- **A doutrina subjetiva**: que considera que os dados são pessoais apenas para quem tem meios razoáveis de os associar a um indivíduo.

Desta forma, é claro que uma aplicação estrita da teoria absoluta leva à conclusão de que os dados são pessoais ou não pessoais em si mesmos, independentemente de quem os tenha em seu poder. Por exemplo, um código pseudonimizado seria um dado pessoal para um indivíduo, mesmo que este não o conseguisse associar a uma pessoa singular, desde que, algures, o responsável pelo tratamento tivesse a "chave" ou tabela de correspondência que permitisse essa reidentificação.

Esta interpretação "monolítica" do conceito de dados pessoais, embora procure proteger particularmente os direitos dos titulares dos dados, origina encargos regulamentares que, por vezes, são insuportáveis para os responsáveis pelo tratamento de dados. Contudo, esta tem sido a interpretação adotada pela maioria das autoridades de controlo da proteção de dados e, consequentemente, pelos operadores, uma vez que implica um menor risco de incumprimento das normas regulamentares para os responsáveis pelo tratamento.

No entanto, mais recentemente, esta conceção tem sido rebatida em acórdãos do TJUE, como nos casos Breyer e Scania. Nestas decisões, o Tribunal opta pela interpretação subjetiva, afirmando, em síntese, que um endereço IP dinâmico (no caso da Breyer) ou um número de identificação do veículo (VIN) (no caso da Scania) constituem dados pessoais apenas na medida em que uma entidade possa associar essa informação a uma pessoa singular.

Embora se pudesse esperar que, com o suporte das referidas decisões do TJUE, a posição subjetiva estivesse plenamente estabelecida e aceite, reduzindo assim a importância da decisão que nos ocupa, não é esse o caso. Algumas autoridades, como o Conselho Europeu de Proteção de Dados, nas suas recentes Diretrizes 1/2025 sobre o conceito de pseudonimização — atualmente disponíveis apenas na sua versão preliminar para consulta pública — continuam a adotar uma abordagem decididamente restritiva, inclinando-se mais para a interpretação absoluta do que para a subjetiva.

É por isso que a decisão do TJUE aqui discutida é tão significativa, pois não só reafirma a interpretação subjetiva da lei, como também declara, pela primeira vez com absoluta clareza, que os dados pessoais pseudonimizados (neste caso, um código alfanumérico relativo a uma pessoa) tratados por um responsável "A" podem ser dados pessoais para "A", mas não para um destinatário "B", se este último não puder (razoavelmente) fazer uma ligação ou reidentificação dos dados.

Isto não só reafirma a interpretação subjetiva da lei, como também tem importantes implicações práticas, detalhadas a seguir.

Implicações práticas

Uma vez que, para o responsável pelo tratamento de dados "A", os dados pseudonimizados serão, em qualquer caso, considerados dados pessoais (uma vez que tem a capacidade de reidentificar o titular dos dados a partir do código alfanumérico), "A" deve cumprir integralmente as normas aplicáveis. Isto implica que, entre outras obrigações, deve:

- dispor de uma base legal (Art.º 6.º do RGPD) para tratar esses dados pessoais, incluindo, quando aplicável, uma base legal suficiente para a sua transferência para um terceiro; e

- informar o titular dos dados sobre o tratamento, em conformidade com os Arts. 13.º ou 14.º do RGPD, conforme o caso, incluindo informação sobre as transferências para os destinatários que receberão os seus dados pessoais. O TJUE aborda esta questão na decisão acima referida, embora, dadas as especificidades do caso, exista alguma margem para interpretação

quanto ao tipo de informação que deve ser prestada aos titulares dos dados sobre os destinatários que não poderão associar os dados pseudonimizados aos titulares.

Relativamente ao cessionário "B", este poderia ser considerado responsável pelo tratamento dos dados para todos os efeitos, caso consiga razoavelmente reidentificar o titular dos dados. Contudo, se o cessionário "B" não for considerado um responsável pelo tratamento ao abrigo da doutrina subjetiva (uma vez que não está a tratar dados pessoais, na sua perspetiva), surgem questões complexas, tais como:

Quais são os direitos do titular dos dados em relação ao destinatário dos dados?

A decisão de referência indica que o titular dos dados pode exercer os seus direitos de proteção de dados tanto contra o cedente como contra o cessionário. Para este último, contudo, poderá ser materialmente impossível responder a pedidos de acesso ou de eliminação de dados, por exemplo, uma vez que a informação não seria considerada pessoal para os seus fins.

Que informação deve então o cedente fornecer aos titulares dos dados relativamente aos cessionários que não conseguem identificar o titular dos dados?

Com o objetivo de simplificar os requisitos de informação para os responsáveis pelo tratamento e evitar confusão entre os titulares dos dados e os destinatários que não os conseguem identificar, pode considerar-se a possibilidade de os cedentes: (i) informarem apenas sobre as categorias de cessionários para os quais a informação recebida não será considerada dados pessoais (sem identificar cada cessionário individualmente); ou (ii) informarem de que determinados destinatários não os poderão identificar com a informação recebida, antecipando assim os problemas identificados. Como se referiu acima, a decisão do TJUE deixa alguma margem para interpretação sobre este ponto (à luz, por exemplo, das bases legais aplicáveis em cada caso).

Isto aplica-se aos subcontratantes para o tratamento?

No caso das relações de subcontratante do tratamento, surgem dúvidas significativas quanto à aplicabilidade desta doutrina nos casos em que o "subcontratante" opera seguindo as instruções do responsável pelo tratamento, mas trata dados pseudonimizados que não constituem dados pessoais para o subcontratante. Neste caso, a prudência sugere que a teoria subjetiva não se aplicaria na sua totalidade, uma vez que, como o subcontratante opera em nome do responsável pelo tratamento, seria difícil argumentar que está a tratar dados "não pessoais" (ao seguir as instruções do responsável, as possibilidades de reidentificação não devem ser consideradas remotas em caso algum). Contudo, este é um caso que justifica um estudo mais aprofundado, uma vez que as implicações práticas da aceitação da plena aplicabilidade da doutrina subjetiva nesta instância seriam substanciais (considere-se a facilidade que traria para a contratação com terceiros).

Conclusões

O acórdão do TJUE no caso *EDPS v SRB* representa não só uma reafirmação da doutrina subjetiva já conhecida, como também um marco importante para os profissionais da área, uma vez que fornece informação altamente relevante sobre a implementação desta doutrina. Em particular:

- Esclarece que os dados pseudonimizados podem ou não ser considerados dados pessoais, dependendo de quem os trata e das possibilidades reais de identificação de pessoas singulares. A decisão fornece também orientações sobre as obrigações dos cedentes e cessionários de dados pseudonimizados, que devem ser estudadas em detalhe para a sua correta implementação.

- Abre um novo território para os profissionais de proteção de dados explorarem, devendo estes considerar as suas conclusões ao estruturar os marcos de conformidade para os responsáveis pelo tratamento e os subcontratantes. Por exemplo, as suas implicações em relação à utilização de informação pseudonimizada para o treino de modelos de IA podem ser de grande interesse para quem detém grandes volumes de dados pessoais, uma vez que podem facilitar a sua comercialização.

- Esta decisão exige uma nova perspetiva não só em relação às novas transferências ou subcontratações a regularizar, mas também uma reformulação das estruturas existentes, que podem ser afetadas por esta interpretação das normas.

2. Comparação da transposição da NIS II por parte de Portugal com a prevista em Espanha

Em julho de 2025, o Governo Português retomou o processo de transposição da Diretiva (UE) 2022/2555 (NIS 2) mediante a apresentação da Proposta de Lei n.º 7/XVII/1. Nesta análise, comparamos esta transposição com o projeto de lei espanhol, analisando as áreas de aplicação, sujeitas e isentas em cada caso, assim como o regime sancionatório previsto.

Manuel Liberal Jerónimo e Luisa Cyrne

A anterior Proposta de Lei (Proposta de Lei n.º 50/XVI/1), caducou com a dissolução da Assembleia da República, a 11 de março. Atualmente, Portugal está ainda em incumprimento do prazo de transposição em outubro de 2024, o que levou à instauração do processo de infração pela Comissão Europeia em novembro do mesmo ano.

Em comparação com a proposta de lei espanhola (***Anteproyecto De Ley De Coordinación Y Gobernanza De La Ciberseguridad***), uma das principais diferenças entre a Proposta de Lei Portuguesa e a espanhola, prende-se com o âmbito de aplicação, designadamente, o seguinte:

ÂMBITO DE APLICAÇÃO SUBJETIVO

Portugal	Espanha
Entidades privadas	**Entidades públicas ou privadas**
• *Dos setores de importância crítica*: Energia; transportes; bancário; infraestruturas do mercado financeiro; saúde; água; infraestruturas digitais[1]; prestadores de serviços geridos; espaço. • *De outros setores críticos:*	

[1] Onde se incluem os fornecedores de pontos de troca de tráfego, os prestadores de serviços de DNS, registos de nomes de TLD, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, fornecedores de redes de distribuição de conteúdos, prestadores de serviços de confiança, fornecedores de redes públicas de comunicações eletrónicas e prestadores de serviços de comunicações eletrónicas acessíveis ao público.

Portugal	Espanha
Serviços postais e de estafeta; gestão de resíduos, produção, fabrico e distribuição de produtos químicos; produção, fabrico e distribuição de produtos alimentares; indústria transformadora; prestação de serviços digitais[2]; investigação. **Espanha acrescenta ainda: os setores da indústria nuclear e da segurança privada.**	
■ Administração Pública; ■ Provedoria de Justiça; ■ Conselho Económico e Social; ■ Serviços técnicos e administrativos da Presidência da República, da Assembleia da República, dos Tribunais, do Conselho Superior da Magistratura, do Conselho Superior dos Tribunais Administrativos e Fiscais e do Conselho Superior do Ministério Público.	■ Entidades da Administração pública, com exclusão do poder judicial, dos parlamentos e dos bancos centrais.
■ Instituições do ensino superior.	■ Universidades e centros de investigação (em assuntos ou projetos de investigação relacionados com os setores críticos)
Entidades críticas (por designar)	

Exclusões do âmbito de aplicação

Portugal	Espanha
■ Estado-Maior General das Forças Armadas e dos ramos das Forças Armadas3; ■ Entidades públicas com responsabilidades de investigação criminal e aos órgãos de polícia criminal e de segurança pública3; ■ Entidades públicas com responsabilidades exclusivas em matéria de produção de informações, nomeadamente ao Sistema de Informações da República Portuguesa, ao Serviço de Informações Estratégicas	■ Entidades da Administração Pública que realizam atividades nas áreas da segurança nacional, defesa nacional ou segurança pública, incluindo a prevenção, investigação, deteção e julgamento de infrações penais, exceto nas atividades em que atuam como prestadores de serviços de confiança disponíveis para terceiros. ■ Instituto de Crédito Oficial.

[2] Onde se incluem os prestadores de serviço de mercados em linha; prestadores de serviço de motores de pesquisa em linha; e prestadores de serviço de plataformas de redes sociais.

[3] No que respeita às redes e sistemas de informação diretamente relacionados com o seu comando e controlo.

Portugal	Espanha
de Defesa e ao Serviço de Informações de Segurança[3]; ■ Entidades públicas cuja atividade incida sobre redes e sistemas de informação diretamente relacionados com a produção e difusão de informação classificada, nomeadamente com as marcas nacionais, da Organização do Tratado do Atlântico Norte (OTAN), e da União Europeia, ou catalogada como segredo de Estado, no que respeita a essas redes e sistemas de informação; ■ Demais entidades públicas que exercem a sua atividade nos domínios da segurança nacional, da segurança pública, da defesa, e dos serviços de informações, no que respeita às redes e sistemas de informação diretamente relacionados com as atividades de produção de informações e prevenção, investigação, deteção e repressão de infrações penais; ■ Entidades privadas que prestem serviços exclusivamente a uma ou mais entidades previstas nas alíneas anteriores e no que respeita a estas atividades.	

Ambas as propostas adotam a mesma metodologia e critérios para a classificação das entidades abrangidas como entidades **essenciais**. A classificação das entidades como entidades **importantes** também assume os mesmos critérios de classificação, sendo que Espanha inclui ainda os municípios que, não sendo municípios de grande população, tenham mais de 20.000 habitantes, e as entidades do seu setor público institucional. Por seu lado, Portugal optou pela inclusão de um artigo dedicado exclusivamente às entidades públicas que não sejam qualificadas como entidades essenciais ou importantes, classificando-as como entidades públicas relevantes e dividindo-as em dois grupos, para efeitos de aplicação de regimes específicos nos termos da proposta e restante regulamentação emitida pelo Centro Nacional de Cibersegurança.

No que diz respeito ao regime sancionatório, também se podem antecipar algumas diferenças:

Regime sancionatório

Contraordenação	Portugal	Espanha
Muito grave	Praticada por entidade essencial: ■ De €2.000,00 a €10.000.000,00 ou a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior; ■ De €350,00 a €200.000,00, se praticadas por uma pessoa singular. Praticada por entidade importante: ■ De €1.250,00 a €7.000.000,00 ou num montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial; ■ De €350,00 a €200.000,00, se praticadas por uma pessoa singular. Praticada por entidade pública relevante (consoante seja integrada no Grupo A ou B): De €8.000,00 a €4.000.000,00.	No geral: €500.001,00 a €2.000.000,00. Praticada por entidade essencial: coima pode ascender €10.000.000,00 ou a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior. Praticada por entidade importante: coima pode ascender a €7.000.000,00 ou um montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial.
Grave	Praticada por entidade essencial: ■ De €1.250,00 a €5.000.000,00 ou a 1 % do volume de negócios anual a nível mundial, no exercício financeiro anterior; ■ De €250,00 a €125.000,00, se praticadas por uma pessoa singular. Praticada por entidade importante: ■ De €875,00 a €3.500.000,00 ou num montante máximo não inferior a 0,7% do volume de negócios anual a nível mundial; ■ De €250,00 a €125.000,00, se praticadas por uma pessoa singular.	No geral: de €100.001,00 a €500.000,00.

Contraordenação	Portugal	Espanha
	Praticada por entidade pública relevante (consoante seja integrada no Grupo A ou B): De €5.000,00 a €225.000,00.	
Leve	De €875,00 a €45.000,00, se praticadas por uma pessoa coletiva; De €250,00 a €3.750,00, se praticadas por uma pessoa singular.	No geral: de €10.000,00 a €100.000,00.

No cômputo geral, as propostas são bastante semelhantes no que diz respeito às obrigações previstas para as entidades abrangidas pelo seu âmbito de aplicação e ambas as propostas refletem um compromisso inequívoco com a melhoria da resiliência cibernética, com realces e nuances que evidenciam as prioridades e modelos institucionais de cada Estado-Membro.

3. Resoluções das autoridades de proteção de dados

Autarquia Local sancionada por enviar comprovativo de pagamento de uma coima para uma morada desatualizada

A Agência Espanhola de Proteção de Dados (AEPD) concluiu o processo sancionatório contra uma Autarquia Local por enviar um comprovativo do pagamento de uma coima de trânsito para a morada desatualizada da reclamanete, onde reside o seu ex-companheiro.

O documento continha os dados pessoais da denunciante, incluindo a matrícula do veículo, a data e o local da infração. A reclamante tinha atualizado a sua morada junto da Direção-Geral de Trânsito (DGT) e informado o agente de fiscalização da Autarquia Local, mas o comprovativo foi enviado para uma morada antiga que constava na base de dados de coimas desde 2013. A Autarquia Local argumentou que o comprovativo não fazia parte do processo sancionatório e que o sistema selecionou automaticamente a morada porque a informação não tinha sido atualizada antes do pagamento.

A AEPD considera que foram violados os princípios da integridade e confidencialidade (Artigo 5.º, n.º 1, alínea f) do RGPD) e da exatidão (Artigo 5.º, n.º 1, alínea d) do RGPD), uma vez que não foram adotadas medidas técnicas e organizacionais adequadas para garantir a segurança e a atualização dos dados. A resolução sublinha que a notificação de uma contraordenação rodoviária entregue pessoalmente, na qual a parte afetada indicou expressamente a sua morada atual, não foi considerada pelo sistema informático na geração do comprovativo de pagamento. Este comprovativo foi enviado automaticamente para uma morada antiga registada na base de dados de coimas, sem que tenha sido efetuada uma consulta atualizada junto da DGT.

Consequentemente, declara-se uma infração muito grave, nos termos do Artigo 83.º, n.º 5, alínea a) do RGPD e do artigo 72.º, n.º 1, alínea a) da LOPDGDD, e determina-se que a resolução seja comunicada ao Provedor de Justiça.

O recurso de uma empresa de telecomunicações contra uma coima por duplicação fraudulenta de cartão SIM foi rejeitado

A Agência Espanhola de Proteção de Dados (AEPD) rejeitou o recurso interposto por uma empresa de telecomunicações contra a resolução sancionatória de 8 de novembro de 2024, que aplicou uma coima de 200.000 euros por violação do Artigo 6.º, n.º 1 do RGPD.

A sanção resultou da emissão fraudulenta de um cartão SIM duplicado a um terceiro, sem base jurídica válido ou o consentimento do titular do cartão. A empresa alegou ter seguido os seus protocolos internos e agido

com diligência, mas a AEPD concluiu que estas medidas foram insuficientes para garantir a legalidade do tratamento. A Agência enfatizou que a responsabilidade pelo tratamento recai sobre o operador, que deve verificar adequadamente a identidade do requerente e garantir que o tratamento está em conformidade com o RGPD. As circunstâncias atenuantes invocadas pela entidade sancionada, como a cooperação com a AEPD, a ausência de benefícios e a não utilização de dados sensíveis, foram rejeitadas por não cumprirem os critérios exigidos. Além disso, a reincidência em infrações semelhantes e a ligação direta entre a atividade comercial e o tratamento de dados pessoais foram considerados fatores agravantes.

A resolução sublinha que a emissão de um cartão SIM a terceiros sem autorização constitui um tratamento ilícito, com potencial para facilitar fraudes graves, como o acesso a contas bancárias ou redes sociais. A AEPD reafirma a necessidade de sanções dissuasoras e eficazes e reitera que a responsabilidade proativa exige não só a implementação de medidas, mas também a garantia da sua eficácia em todos os momentos.

Uma rede de centros comerciais foi sancionada por várias violações de dados pessoais e medidas de segurança

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma rede de centros comerciais com três coimas que ascendem a um total de 3.200.000 euros por violações do Regulamento Geral de Proteção de Dados (RGPD).

A resolução decorre de cinco violações de segurança reportadas entre janeiro e setembro de 2023, afetando um total de 118.895 pessoas. Os ataques, realizados com recurso a técnicas de *credential stuffing*, permitiram o acesso não autorizado a dados pessoais como o nome, morada, e-mail, data de nascimento e credenciais de login. A AEPD concluiu que a entidade infringiu o Artigo 5.º, n.º 1, alínea f) do RGPD (princípio da integridade e confidencialidade), o Artigo 32.º (segurança do tratamento) e o Artigo 34.º (comunicação das violações aos titulares dos dados).

A empresa alegou ter adotado medidas técnicas e organizacionais, como auditorias e autenticação de dois fatores, mas a AEPD considerou que estas foram tardias, insuficientes ou implementadas incorretamente. Além disso, verificou-se que as comunicações enviadas aos afetados não cumpriam os requisitos do Artigo 34.º do RGPD, uma vez que omitiam informações essenciais sobre a natureza da violação e as medidas tomadas.

A AEPD considerou a dimensão dos dados comprometidos, a negligência na gestão da segurança e a ligação direta entre a atividade comercial e o tratamento massivo de dados pessoais como fatores agravantes.

Empresa de eletricidade e gás sancionada por contratação de serviços fraudulenta

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma empresa de eletricidade e gás com uma coima de 100.000 euros por violar o Artigo 6.º, n.º 1 do Regulamento Geral sobre a Proteção de Dados (RGPD) ao tratar ilegalmente dados pessoais sem base legal.

A denúncia foi feita por um indivíduo que relatou ter sido inscrito em contratos de gás, eletricidade e serviços relacionados sem o seu consentimento. A entidade sancionada alegou que o contrato era gerido por uma empresa colaboradora, atuando como subcontratante para o tratamento, e que esta empresa agiu de forma fraudulenta e extravasando as suas instruções.

No entanto, a AEPD concluiu que a empresa não exerceu um controlo adequado sobre a sua subcontratante, falhando no seu dever de supervisão e permitindo o tratamento de dados sem fundamento jurídico. Embora os contratos e as faturas tenham sido cancelados

na sequência da denúncia, a Agência considerou que a empresa não demonstrou ter agido com a devida diligência. A resolução sublinha que o responsável pelo tratamento de dados pode ser sancionado pelas ações dos seus subcontratantes para o tratamento quando o cumprimento do RGPD não é garantido.

A infração foi classificada como muito grave, nos termos do Artigo 72.º, n.º 1, alínea b), da Lei Espanhola de Proteção de Dados (LOPDGDD). A AEPD considerou a natureza do tratamento, o volume de dados afetados e a ligação da atividade empresarial ao tratamento massivo de dados pessoais como fatores agravantes.

Coima de 200.000 euros para fornecedor de energia por inscrever um cliente num registo de devedores antes de a notificação de cobrança ser devolvida

A Agência Espanhola de Proteção de Dados (AEPD) aplicou uma sanção de 200.000 euros a um fornecedor de energia por inscrever os dados de um cliente num registo sem cumprir os requisitos do Artigo 20.º, n.º 1 da Lei Espanhola de Proteção de Dados (LOPD-gdd), o que configura um tratamento de dados sem fundamento legítimo, de acordo com o Artigo 6.º, n.º 1 do RGPD.

O reclamante alegou não ter recebido qualquer notificação de cobrança nem informação sobre a sua eventual inclusão em registos de incumpridores. Apesar de a reclamada ter enviado a notificação de cobrança, esta foi devolvida pelos Correios numa data posterior à inscrição no registo de devedores, demonstrando que esta foi realizada sem confirmação de receção ou devolução da notificação. Por conseguinte, a AEPD conclui que a obrigação de informar previamente a parte afetada, conforme exigido pelo Artigo 20.º, n.º 1, alínea c), não foi cumprida. Esta disposição estipula que essa advertência seja feita no contrato ou no momento do pedido de pagamento.

A sanção é agravada pela natureza da infração, que afetou a solvência do reclamante; pela ligação entre a atividade da reclamada e o tratamento de dados pessoais; e pela negligência na inclusão dos dados quando a dívida não cumpria os requisitos legais.

Uma empresa de telecomunicações na Alemanha é sancionada por falhas de controlo e segurança

A Autoridade Federal Alemã de Proteção de Dados aplicou duas sanções administrativas num total de 45 milhões de euros, a uma empresa de telecomunicações, além de uma advertência, devido a graves deficiências na supervisão dos subcontratantes para o tratamento e na segurança do seu portal de serviços online.

A reclamada, que opera através de lojas físicas geridas por agências parceiras que atuam como subcontratantes para o tratamento, tinha contratos de subcontratação do tratamento, embora estes não fossem devidamente controlados e auditados. Isto originou vulnerabilidades nos sistemas informáticos que facilitaram a utilização indevida de dados pessoais em casos de fraude. Deste modo, aplicou-se uma coima de 15 milhões de euros e uma advertência por controlo insuficiente e fragilidades técnicas.

Além disso, a entidade foi sancionada em mais 30 milhões de euros por falhas nos mecanismos de autenticação do seu portal online, que, combinadas com o suporte telefónico, permitiram a utilização indevida de eSIMs.

A Agência Espanhola de Proteção de Dados (AEPD) concluiu que o direito à portabilidade dos dados não se aplica ao setor público da educação, mas aceitou uma queixa referente ao atraso na resposta

A reclamante apresentou queixa contra a Secretaria de Educação da Junta de Castela e Leão, alegando que o seu direito à

portabilidade dos dados das suas filhas, alunas de diferentes escolas públicas, tinha sido desrespeitado, uma vez que não recebeu qualquer resposta dessas escolas no prazo de um mês estabelecido por lei. Em concreto, os dados diziam respeito às avaliações psicopedagógicas das filhas, realizadas entre 2018 e 2023.

A este propósito, a reclamante defende que os centros educativos do Governo Regional dispõem de plataformas eletrónicas que permitem a transmissão direta de dados de um responsável para outro, podendo, por isso, o Governo Regional disponibilizar a referida documentação através do sistema de notificação eletrónica. Por sua vez, a reclamada afirma que a documentação solicitada está à disposição da reclamante nos respetivos centros educativos, uma vez que não pode enviar dados de saúde para endereços de correio eletrónico privados, como é o caso do centro de psicologia privado para o qual está a ser pedida a portabilidade.

Na sua resolução, a AEPD entende que, uma vez que a relação (escola pública-pais) é administrativa e não contratual, sendo, por isso, regulada pela legislação do ensino público, o direito à portabilidade de dados não se aplica neste caso, com base no considerando 68 e no Artigo 20.º do RGPD.

i. O considerando 68 do RGPD estabelece que "esse direito não deverá ser exercido em relação aos responsáveis pelo tratamento que tratem dados pessoais na prossecução das suas atribuições públicas. Por conseguinte, esse direito não deverá ser aplicável quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de atribuições de interesse público ou para o exercício da autoridade pública de que esteja investido o responsável pelo tratamento."

ii. Artigo 20.º do RGPD: "tal direito não se aplicará ao tratamento que for necessário para o cumprimento de uma missão realizada por interesse público ou no exercício de poderes públicos conferidos ao responsável pelo tratamento."

A AEPD conclui que o direito à portabilidade dos dados não é aplicável neste caso, mas acolhe a reclamação por razões formais, uma vez que a resposta foi emitida tardiamente. No entanto, reconhece que não é necessária qualquer outra ação por parte da reclamada.

Um trabalhador foi multado em 300 euros por tratar dados pessoais sem qualquer fundamento legal

Inicialmente, uma pessoa singular apresentou queixa contra uma loja de frutas e legumes depois de ter sido contactada através de mensagens pessoais do WhatsApp por um trabalhador da empresa. A reclamante entendeu que o trabalhador obteve os seus dados a partir de informações que forneceu para a gestão do cartão "Salamanca Tarjeta Activa", utilizado para obter descontos em estabelecimentos locais.

Durante o processo de alegações, a empresa afirmou ter obtido os dados diretamente da reclamante, argumentando que esta é uma cliente frequente que faz encomendas específicas para as quais necessita de ser contactada, e que a reclamante participa ativamente num sorteio de Natal para o qual é necessário o fornecimento dos seus dados. No entanto, embora a reclamação tenha sido inicialmente rejeitada, a reclamante interpôs recurso, negando categoricamente as alegações da parte contrária, enfatizando a natureza pessoal das mensagens enviadas e apontando a falta de provas do alegado pela arguida.

A Agência Espanhola de Proteção de Dados (AEPD) aceitou o recurso e ordenou a continuação do processo, decidindo realizar uma investigação para determinar a autoria e a origem do tratamento dos dados. A este respeito, a AEPD determinou que a pessoa que contactou o reclamante era, de facto, um trabalhador da empresa, que o fez a partir de um telemóvel pessoal e que, além disso, a origem dos dados, como alegado pela reclamante, era a transferência de dados da

plataforma que geria o cartão "Salamanca Tarjeta Activa" para as empresas aderentes, incluindo a reclamada.

Por isso, a AEPD decide promover um procedimento sancionador e, à luz dos factos, conclui que o trabalhador utilizou os dados pessoais que a reclamante tinha fornecido à entidade reclamada por motivos profissionais e não por motivos pessoais. Consequentemente, deduz-se que o trabalhador agiu a título pessoal e não em nome da entidade empregadora ou a seguir instruções desta, o que significa que as operações de tratamento realizadas não podem ser justificadas pela base contratual em que a entidade se fundamenta. Por fim, a AEPD decide aplicar ao trabalhador uma coima de 300 euros por violação do Artigo 6.º, n.º 1 do RGPD, tipificada no Artigo 83.º, n.º 5, alínea a) do RGPD.

A Agência Espanhola de Proteção de Dados (AEPD) decidiu arquivar uma reclamação pela instalação de um visor digital por não existir infração em matéria de proteção de dados

A 19 de junho de 2025, a AEPD resolveu um procedimento decorrente de uma reclamação apresentada por um morador de um condomínio contra outro, alegando que este tinha instalado um visor digital na sua porta sem autorização prévia do condomínio. O denunciante afirmou ainda que o dispositivo era capaz de gravar imagens de zonas comuns e que não estava devidamente sinalizado.

A AEPD decidiu arquivar o procedimento adotando critérios gerais relativos aos visores digitais: (i) são permitidos desde que desempenhem uma função semelhante à de um visor tradicional; (ii) não é necessário solicitar autorização ao condomínio para a sua instalação; (iii) a área que abrangem (patamares) não faz parte da esfera privada de uma pessoa, sendo áreas de mera passagem; (iv) os visores digitais geralmente não armazenam quaisquer dados, pelo que não é obrigatório indicar a sua presença através de sinalização. Tudo isto acresce ao facto de as provas apresentadas se terem revelado insuficientes para refutar a presunção de inocência do reclamado.

Uma empresa farmacêutica finlandesa foi multada em 1,1 milhões de euros por deficiências na proteção de dados na sua loja online

A empresa farmacêutica sancionada utilizava cookies e outras tecnologias de rastreio na sua farmácia online, que transmitiam diretamente pacotes de dados dos utilizadores para empresas como a Meta e a Google. Estes dados incluíam interações com diversos medicamentos sujeitos e não sujeitos a receita médica, bem como endereços IP e outras informações que poderiam identificar os utilizadores.

Assim, se um utilizador estivesse ligado à sua conta Google ou Facebook enquanto utilizava a farmácia online, o Google e a Meta poderiam tê-lo identificado diretamente. Isto é particularmente relevante dada a natureza sensível dos dados, uma vez que se relacionam com a saúde das pessoas.

Neste sentido, a autoridade finlandesa considera que a empresa infringiu os artigos 5.º, 25.º e 32.º do RGPD devido à falta de medidas técnicas e organizacionais adequadas e aplicou uma sanção administrativa à empresa farmacêutica sob a forma de uma coima de 1,1 milhões de euros.

Uma pessoa singular foi multada por instalar câmaras apontadas para a casa de um vizinho

A Agência Espanhola de Proteção de Dados (AEPD) multou um particular por instalar câmaras de videovigilância apontadas para a entrada principal e para a piscina da propriedade vizinha. A denúncia data de há mais de quatro anos, quando a parte afetada denunciou à AEPD que a presença das câmaras constituía uma invasão da sua privacidade. Em 2019, o reclamante tentou,

sem sucesso, resolver a questão através da autarquia competente. Posteriormente, a AEPD tentou solicitar informações à pessoa singular sobre as medidas tomadas, mas a notificação não foi entregue devido a problemas de entrega. Finalmente, em setembro de 2024, foi iniciado o processo sancionatório.

A pessoa reclamada alegou que as câmaras instaladas no exterior da sua casa não tinham capacidade de gravação nem serviço de videovigilância, e que o seu único propósito era dissuadir roubos ou vandalismo. Uma inspeção realizada pelos Mossos d'Esquadra (polícia catalã) confirmou que as câmaras não estavam a funcionar.

No entanto, na sua decisão a AEPD adverte que a mera possibilidade de captar imagens de espaços alheios, mesmo que não gravadas, constitui um tratamento de dados pessoais e considera que esta situação afeta a privacidade dos envolvidos, cria uma perceção de vigilância e representa uma medida desproporcionada, uma vez que não se limita à proteção da propriedade alheia. Consequentemente, a AEPD conclui que houve violação do Artigo 5.º, n.º 1, alínea c) do RGPD e, por conseguinte, aplica uma coima de 500 euros.

Empresa de logística multada em 100 mil euros por exigir verificação excessiva de antecedentes criminais e dados pessoais em processos de seleção

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma empresa de logística, armazenamento e transporte de mercadorias em 100 mil euros por exigir informações indevidas aos candidatos durante os processos de seleção. Um queixoso denunciou que, para agendar uma entrevista de emprego, foi-lhe pedido que apresentasse um certificado de registo criminal e que preenchesse um formulário com a indicação do seu estado civil e o número de filhos.

A empresa em causa argumentou que o pedido do certificado era justificado pelo Regulamento de Execução (UE) 2015/1998, que obriga à verificação de antecedentes criminais para os colaboradores com acesso a zonas de carga aérea, e que foi solicitada informação sobre o estado civil e dependentes para preencher o Formulário 145 da Agência Tributária Espanhola (AEAT), referente à declaração de rendimentos do trabalho. No entanto, na sua resolução a AEPD considera que a legislação europeia autoriza a verificação de antecedentes criminais apenas para os candidatos selecionados para o cargo, e não para todos os candidatos na fase de entrevista. Por conseguinte, a prática de solicitar este certificado a todos os candidatos constitui um processamento massivo e injustificado de dados relativos a condenações criminais. Por fim, em relação aos dados solicitados no Formulário 145, a Agência esclarece que os mesmos só devem ser recolhidos após a formalização da relação laboral, e não durante o processo de seleção.

Assim sendo, a AEPD conclui que a empresa violou o Artigo 5.º, n.º 1, alínea c) do RGPD (relativo ao princípio da minimização de dados), bem como o Artigo 10.º do mesmo Regulamento e o Artigo 10.º da Lei Espanhola de Proteção de Dados (LOPD-gdd), no que diz respeito ao tratamento de dados criminais. Por isso, impõe duas sanções: Coima de 75.000 euros por solicitação indevida de antecedentes criminais e coima de 25.000 euros por recolha prematura de dados pessoais

Entidade multada em 32.000 euros por divulgar dados médicos de um trabalhador a um terceiro

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma entidade de prevenção de riscos profissionais em 40.000 euros, valor reduzido para 32.000 euros por pagamento voluntário, por violação do princípio da confidencialidade no tratamento de dados pessoais, nos termos do Artigo 5.º, n.º 1, alínea f) do RGPD.

O processo teve início após uma denúncia de um trabalhador que, ao aceder ao seu relatório médico através da plataforma online

do serviço de prevenção, descobriu que o documento incluía registos médicos pertencentes a outro trabalhador. O incidente ocorreu devido a um erro no processo de digitalização e carregamento do documento, que permitiu o acesso não autorizado a informação particularmente sensível.

A AEPD determinou que a entidade não implementou medidas organizacionais adequadas para prevenir tais situações, resultando na perda de controlo sobre os dados pessoais por parte do titular dos dados. Embora a empresa tenha alegado que se tratava de um erro humano e apresentado medidas corretivas como formação de pessoal, revisão de protocolos e certificações de segurança, a Agência concluiu que estas ações foram adotadas a posteriori e não a isentavam de responsabilidade.

A infração foi classificada como muito grave, já que afetou dados de saúde, considerados especialmente protegidos pela legislação. Embora tenha sido inicialmente considerada uma possível violação do Artigo 32.º do RGPD (segurança do tratamento), esta hipótese foi descartada, uma vez que a ausência de medidas técnicas gerais não pôde ser comprovada.

Uma organização foi multada em 180.000 euros por incumprimento da decisão final da AEPD

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma organização em 225.000 euros, valor reduzido para 180.000 eurosmediante pagamento voluntário, por incumprimento de uma decisão final que a obrigava a cumprir o direito de acesso de um titular de dados, conforme oArtigo 15.º do RGPD.

O processo teve início após a organização se ter recusado repetidamente a responder aos pedidos da AEPD, que exigia o fornecimento ao requerente de um certificado de acesso ou de uma justificação fundamentada da recusa, no prazo de dez dias úteis. Apesar dos múltiplos pedidos realizados entre março e outubro de 2024, a empresa não demonstrou o cumprimento da decisão, o que levou a AEPD a instaurar um processo sancionatório por violação do Artigo 58.º, n.º 2 do RGPD, que exige o cumprimento das ordens da autoridade de supervisão.

A entidade alegou confusão entre procedimentos semelhantes e falta de intenção de violar a lei, mas a AEPD rejeitou estas justificações, reiterando que o cumprimento das decisões finais é obrigatório, independentemente de erros internos. Além disso, a AEPD classificou a infração como muito grave, nos termos do Artigo 72.º, n.º 1, alínea m) da LOPD-gdd, e enfatizou a importância do princípio da responsabilidade proativa, que obriga o responsável pelo tratamento de dados a garantir e demonstrar a conformidade com o RGPD ao longo de todo o ciclo de vida do tratamento.

A penalização foi graduada tendo em conta fatores como a duração da não conformidade (mais de um ano), os repetidos pedidos de informação e o facto de ter afetado apenas um titular de dados. Por fim, a entidade optou pelo pagamento voluntário, o que permitiu o encerramento antecipado do processo.

A Agência Espanhola de Proteção de Dados (AEPD) defende a conservação de dados pessoais por um subcontratante do tratamento após o termo da subcontratação

Neste caso, um subcontratante para o tratamento opunha-se à eliminação dos dados pessoais objeto da subcontratação, uma vez terminada a relação contratual com o responsável pelo tratamento de dados. Em vez disso, o subcontratante manteve os dados bloqueados, alegando que tal era necessário para garantir o exercício adequado do seu direito de defesa dos seus legítimos interesses, uma vez que se encontrava envolvido num litígio com o responsável pelo tratamento dos dados.

Na sua decisão, a AEPD considera que o Artigo 33.º, n.º 4 da LOPD-gdd suporta esta opção, ao estabelecer: “O subcontratante para o tratamento pode conservar os dados,

devidamente bloqueados, enquanto existirem responsabilidades decorrentes da sua relação com o responsável pelo tratamento de dados", pelo que, conjugando esta disposição com o direito a uma tutela jurisdicional efetiva, a AEPD decidiu arquivar o processo.

Embora a AEPD não se aprofunde em conceitos interessantes que surgem na resolução — como o de bloqueio — nem especifique as implicações regulatórias da retenção desses dados pelo subcontratante fora do âmbito do contrato de tratamento (por exemplo, referindo-se ao seu papel nesse momento, ao dever de informar os titulares dos dados, às bases legais aplicáveis nesse contexto, etc.), trata-se de uma resolução que merece ser considerada, pois traz à tona uma questão muito comum na prática, mas pouco discutida no setor: a autorização prevista no Artigo 33.º, n.º 4 da LOPD-gdd.

A Agência Espanhola de Proteção de Dados (AEPD) considera que, para cumprir o Artigo 28.º do RGPD, não basta declarar no DPA que os dados serão apagados ou devolvidos após a conclusão do tratamento

Numa sanção resultante de uma violação de segurança sofrida por um subcontratante para o tratamento que presta serviços ao responsável pelo tratamento de dados, a AEPD considera insuficiente a cláusula genérica normalmente incluída nos contratos de tratamento de dados, segundo a qual o subcontratante é obrigado a apagar ou devolver os dados após o fim do serviço.

A este respeito, a AEPD considera que o responsável pelo tratamento deve, caso não esteja expressamente previsto no contrato, fornecer instruções claras e operacionais para que o subcontratante respeite os mesmos prazos de retenção aplicáveis ao responsável pelo tratamento, de modo a que o subcontratante não retenha todos os dados até ao termo do contrato, quando já não forem necessários.

A resolução impõe uma coima de 250.000 euros ao responsável pelo incumprimento do Artigo 5.º, n.º 1, alínea f) do RGPD e outra de 50.000 euros pelo incumprimento do Artigo 28.º do RGPD.

A autoridade de controlo francesa multa a Google e a Shein por instalarem cookies e tecnologias semelhantes sem consentimento

A CNIL francesa aplicou duas sanções históricas: 325 milhões de euros à Google e 150 milhões de euros à Shein, no âmbito do seu plano de ação sobre *cookies* e publicidade digital.

No caso da Google, a autoridade constatou que a empresa inseria anúncios no formato de e-mail nos separadores "Promoções" e "Social" do Gmail sem obter o consentimento prévio dos utilizadores, o que configura um prospeção eletrónica proibida pela legislação francesa. Além disso, o processo de criação da conta Google não garantia o consentimento válido para a instalação de cookies de publicidade, dado que a informação fornecida era insuficiente e a opção de recusa era difícil.

Por sua vez, a Shein foi sancionada por instalar cookies de publicidade nos dispositivos dos utilizadores antes de estes poderem dar o seu consentimento e por utilizar banners informativos incompletos que não explicavam adequadamente os objetivos da publicidade nem identificavam os terceiros envolvidos. A CNIL constatou ainda que, mesmo após a rejeição dos cookies ou a retirada do consentimento, os rastreadores continuavam a ser instalados e lidos.

Ambas as resoluções realçam a importância de obter o consentimento prévio, livre e informado antes de qualquer tratamento de dados para fins publicitários, além de oferecer mecanismos de recusa tão acessíveis como os de aceitação. A CNIL alerta que continuará a monitorizar ativamente o cumprimento das normas, especialmente no que diz respeito a práticas enganosas ou desproporcionais no

design de *banners* e formulários de consentimento dos utilizadores.

A Agência Espanhola de Proteção de Dados (AEPD) não aprova a utilização de fotografias de trabalhadores para controlo de assiduidade

A AEPD está a analisar a legalidade do sistema de controlo de ponto implementado pela RENFE INGENIERÍA Y MANTENIMIENTO SME, S.A., que combina a utilização de um crachá de identificação com a captura de uma fotografia no momento do registo de entrada, diferenciando entre a sede (apenas o crachá) e os centros de manutenção (crachá e fotografia).

De acordo com o Artigo 4.º do RGPD, uma fotografia constitui um dado pessoal, mas não é um dado biométrico, uma vez que não são utilizados meios técnicos específicos para a identificação automática, sendo a verificação feita manualmente pelo Departamento de Recursos Humanos. É examinada a conformidade com os princípios do Artigo 5.º do RGPD, em particular os da licitude, minimização de dados, limitação da finalidade e segurança, bem como a base jurídica para o registo do horário de trabalho, que é o cumprimento de uma obrigação legal, a prevenção de fraude e a gestão da relação contratual através do acompanhamento da atividade laboral (Artigos 20.º, n.º 3 e 34.º, n.º 9 do Estatuto dos Trabalhadores).

Verifica-se que a informação fornecida aos trabalhadores é adequada e que o tratamento é necessário e proporcional, descartando métodos alternativos mais intrusivos. Assim sendo, não se verifica qualquer infração, uma vez que o sistema não viola os princípios do RGPD nem envolve o tratamento de dados biométricos, sendo o processo encerrado.

Um clube de futebol foi sancionado por uma violação de segurança causada por um ataque de 'ransomware'

A Agência Espanhola de Proteção de Dados (AEPD) sancionou um clube de futebol por uma violação de segurança causada por um ataque de *ransomware* que afetou os dados pessoais de aproximadamente 60.000 pessoas, incluindo dados especialmente protegidos.

A AEPD fundamenta a sua competência no Artigo 58.º, n.º 2 do RGPD e naLOPD-gdd, e sublinha que a entidade, enquanto responsável pelo tratamento de dados, deve garantir a integridade e a confidencialidade dos dados (Artigo 5.º, n.º 1, alínea f) do RGPD), além de implementar medidas técnicas e organizacionais adequadas ao risco (Artigo 32.º do RGPD).

A resolução confirma a falta de medidas suficientes, como a ausência de segmentação de rede e encriptação de dados, o que permitiu ao ataque comprometer todos os servidores virtualizados e backups. A gravidade da infração é salientada devido ao volume e à sensibilidade dos dados afetados, bem como à duração da infração.

A conduta é classificada como uma infração muito grave (Artigo 83.º, n.º 5 do RGPD e Artigo 72.º da LOPD-gdd) e uma infração grave (Artigo 83.º, n.º 4 do RGPD e Artigo 73.º da LOPD-gdd), sendo aplicada uma coima total de 110.000 euros, reduzida para 66.000 euros mediante reconhecimento de responsabilidade e pagamento voluntário. Além disso, foram determinadas medidas corretivas para adequar a segurança ao RGPD.

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma empresa tecnológica por transferir dados pessoais para terceiros sem fundamento jurídico suficiente

A reclamante, uma associação que promove a democracia e os direitos digitais, apresentou uma queixa à AEPD contra uma empresa tecnológica, alegando que os dados pessoais de trabalhadores independentes fornecidos à Agência Tributária Espanhola (AEAT) e ao Registo Comercial para inscrição no censo de

atividades económicas foram posteriormente tratados e transferidos para terceiros — incluindo a Câmara de Comércio, a Camerdata e consultoras privadas — para fins comerciais e de marketing, sem base legal suficiente e sem que os titulares dos dados tivessem sido devidamente informados. A reclamação enfatizou que estes dados, que incluíam identificadores como números de identificação fiscal (NIF), foram disponibilizados online e utilizados para fins diferentes dos inicialmente comunicados.

Durante a investigação, a AEPD recolheu informações das entidades envolvidas. A empresa defendeu a legalidade do tratamento invocando o interesse legítimo, a origem dos dados em fontes públicas e a adoção de medidas indiretas de informação. No entanto, a AEPD concluiu que o tratamento de dados excedia o enquadramento legal estabelecido na Lei 4/2014 sobre Câmaras de Comércio, uma vez que se destinava à comercialização em massa de bases de dados para campanhas de marketing, e que a presunção de licitude prevista no Artigo 19.º da LOPD-gdd não abrangia a utilização de dados de identificação, como o NIF. Além disso, constatou uma violação do dever de informação previsto no Artigo 14.º do RGPD, uma vez que não foi assegurado que os titulares dos dados fossem efetivamente informados.

Consequentemente, a AEPD aceitou a reclamação, declarou violados os artigos 6.º, n.º 1 e 14.º do RGPD, aplicou coimas de 24.000 e 18.000 euros, respetivamente, e ordenou a cessação do tratamento e a eliminação dos dados tratados sem fundamento legítimo.

Uma empresa de viagens foi multada por violar o princípio da minimização de dados

A decisão resulta de uma reclamação apresentada à Agência Espanhola de Proteção de Dados (AEPD) contra uma empresa de viagens. A queixa alegava que a empresa tinha solicitado indevidamente uma cópia integral dos documentos de identidade dos hóspedes durante o processo de check-in online para reservas de alojamento, o que, na visão do reclamante, constituía um pedido excessivo de dados pessoais.

Em concreto, o reclamante alegou que, embora tenha fornecido os dados de identificação necessários, a empresa insistiu na necessidade em enviar uma cópia integral do documento de identidade, alegando ser essencial para cumprir as obrigações legais relativas ao registo e à comunicação às autoridades de segurança. A empresa argumentou que solicitou uma imagem integral dos documentos de identidade dos hóspedes no âmbito do processo de verificação de identidade, em conformidade com o Real Decreto 933/2021, justificando-se com a alegação de que a verificação presencial não era viável no seu modelo de negócio digital.

No entanto, a AEPD, após análise da legislação aplicável e do princípio da minimização de dados do RGPD, considerou que o pedido de uma cópia integral do documento de identidade excedia os dados estritamente necessários para o fim pretendido, uma vez que a legislação apenas exige a recolha de determinados dados de identificação e não uma cópia integral do documento. Consequentemente, a AEPD julgou procedente a reclamação, constatando que a reclamada violou o princípio da minimização de dados estipulado no Artigo 5.º, n.º 1, alínea c) do RGPD, e aplicou uma coima de 70.000 euros, que foi reconhecida e paga voluntariamente pela reclamada, reduzindo-a, assim, para 42.000 euros. Exigiu ainda que a empresa adotasse medidas corretivas para adaptar os seus procedimentos, eliminando a exigência de fornecimento de uma cópia do documento de identidade e eliminando as imagens já recolhidas.

A Autoridade polaca de proteção de dados aplica coimas tanto ao responsável pelo tratamento como ao subcontratante por negligência na análise de riscos e na

implementação de medidas de segurança

A Autoridade de Proteção de Dados da Polónia sancionou uma cadeia de restaurantes em 4.022.773 euros e um dos seus subcontratantes para o tratamento em 43.680 euros após ter constatado graves deficiências na análise de riscos e na implementação de medidas de segurança para o tratamento de dados pessoais.

O caso teve origem na notificação de uma violação de segurança que expôs dados sensíveis de funcionários e franchisados num ficheiro acessível ao público. A investigação revelou que nem o responsável pelo tratamento nem o subcontratante realizaram uma análise de riscos adequada ou implementaram medidas técnicas e organizacionais proporcionais à natureza e à escala do tratamento, incumprindo, assim, os artigos 24.º, 25.º, 28.º, 32.º e 38.º do RGPD. Além disso, o subcontratante subcontratou serviços sem o contrato de subcontratação exigido, e o encarregado da proteção de dados não esteve adequadamente envolvido na gestão da segurança, o que limitou a capacidade preventiva da organização.

A resolução sublinha a importância de uma monitorização eficaz, da atualização contínua das medidas de segurança e do envolvimento ativo do encarregado da proteção de dados em todos os processos relacionados com a proteção de dados.

4. Acórdãos

A Audiência Nacional avalia uma sanção da AEPD por tratamento sem base legal ao publicar listas com nomes e apelidos de candidatos

A Audiência Nacional confirmou a sanção de 12.000 euros aplicada a uma sociedade pela Agência Espanhola de Proteção de Dados (AEPD) em agosto de 2022 por publicar no seu site listas de resultados de um concurso público realizado pelo Serviço Galego de Saúde (SERGAS), incluindo nomes e apelidos, sem o consentimento dos afetados.

O litígio ocorreu porque na publicação realizada pela entidade foram alteradas as listas provisórias de pontuação do processo de seleção para o Grupo Auxiliar da Função Administrativa do SERGAS, que tinham sido publicadas oficialmente pela agência em 2019. Enquanto as listas originais estavam organizadas alfabeticamente e misturavam diferentes turnos, a entidade sancionada reorganizou os dados por pontuação e classificou-os em três categorias: "Acesso Livre", "Incapacidade Geral" e "Promoção Interna". Estas listas incluíam os nomes e apelidos dos candidatos, o que, segundo a AEPD, constitui um tratamento indevido de dados pessoais, uma vez que não está em consonância com as finalidades legítimas da publicação original.

O acórdão rejeitou os argumentos da empresa relativos à anonimização, ao interesse legítimo e à proporcionalidade da sanção, concluindo que as suas ações não estavam abrangidas pela regulamentação, uma vez que envolviam tratamento adicional de dados sem base legal adequada. De acordo com a decisão, a alteração do formato original dos dados pessoais e a sua classificação por pontuação, em vez de seguir a ordem alfabética oficialmente estabelecida, alteraram a finalidade original do tratamento, violando os princípios do RGPD. Em particular, o Tribunal salientou que não houve consentimento explícito dos titulares dos dados nem qualquer outro fundamento jurídico válido para legitimar esta reconfiguração dos dados pessoais.

Consequentemente, a decisão rejeita o recurso contencioso-administrativo interposto pela entidade sancionada e confirma integralmente a deliberação da AEPD, que aplicou a coima de 12.000 euros anteriormente referida.

O TSJ da Galiza analisa a utilização de algoritmos em processos de seleção e confirma a discriminação sindical numa autoridade portuária

Esta decisão do Tribunal Superior de Justiça da Galiza resolve um recurso interposto por uma autoridade portuária contra uma sentença proferida por um Tribunal Social relativamente a uma ação de proteção de direitos fundamentais iniciada por um particular. Em concreto, o caso questiona

se a entidade violou o direito fundamental à liberdade sindical em processos relacionados com a mobilidade funcional e o acesso a determinados cargos dentro da organização, no âmbito da utilização de algoritmos preditivos.

Em 2017, a autoridade portuária aplicou critérios de mobilidade funcional para preencher temporariamente diferentes vagas, utilizando um sistema de perfis e escalas técnicas para selecionar os candidatos, tendo em conta fatores como a distância técnica para o perfil ideal do cargo.

A autora alegou discriminação sindical durante estes processos, uma vez que, embora tenha figurado em diversas ocasiões como a candidata mais adequada de acordo com os critérios objetivos de avaliação, a empresa optou por selecionar outros trabalhadores. Segundo a autora, as decisões foram rejeitadas ou alteradas com base em considerações subjetivas de outros fatores, como a influência dos cargos sindicais. Argumentou que a sua função como secretária da Comissão de Trabalhadores e a sua filiação sindical a prejudicaram.

A entidade arguida não conseguiu provar os verdadeiros motivos para o desvio dos critérios algorítmicos. Por conseguinte, o tribunal declarou que a entidade tinha de facto violado o direito fundamental à liberdade sindical, anulando a nomeação de um dos candidatos selecionados e reconhecendo o direito da autora a receber as diferenças salariais correspondente ao cargo a que legalmente tinha direito. Perante esta decisão, a autoridade portuária interpôs recurso, levando o caso a uma segunda instância para revisão. Esta segunda instância reafirmou que houve discriminação sindical contra a autora.

Em suma, o acórdão estabelece um precedente importante no que diz respeito à garantia dos direitos fundamentais no local de trabalho, particularmente no que respeita à liberdade sindical e à transparência nos processos de seleção interna nas organizações públicas.

A Corte Suprema do Chile ordena que empresa de telecomunicações indemnize cliente por violação de dados pessoais

A Corte Suprema do Chile ordenou que uma empresa de telecomunicações pague sete milhões de pesos de indemnização a um cliente cuja identidade foi utilizada por burlões para contratar cinco linhas telefónicas sem o seu consentimento. A decisão determinou que a empresa falhou no seu dever de proteger os dados pessoais do cliente afetado, facilitando assim a fraude. A empresa foi responsabilizada por não verificar adequadamente a identidade de quem celebrou os contratos, violando a Lei de Proteção de Dados Pessoais.

A decisão estabelece um precedente na proteção de dados pessoais no Chile, sancionando a empresa por violar a lei e facilitar a fraude.

Caso Latombe: O TGUE mantém o regime de transferência internacional UE-EUA

O Tribunal Geral da União Europeia (TGUE) proferiu o seu acórdão no conhecido “Caso Latombe”, relativo a um recurso de anulação apresentado pelo eurodeputado Philippe Latombe contra o atual regime de transferências internacional para os EUA.

Um dos principais pontos deste acórdão gira em torno da independência do Data Protection Review Court (DRPC) dos EUA, que atuaria como tribunal de recurso em matéria de proteção de dados naquela jurisdição. Segundo Philippe Latombe, este DPRC não opera de forma imparcial ou independente devido à sua dependência do poder executivo. No entanto, o TGUE considera que o

DPRC opera ao abrigo de um conjunto de garantias e de acordo com determinadas regras que fornecem provas suficientes da independência funcional dos seus membros. Assim, a par de outras considerações adicionais, o TGUE indeferiu o recurso.

Com esta decisão, o TGUE ratificou, no essencial, o referido regime, confirmando que este oferece garantias suficientes para assegurar um nível adequado de proteção dos dados transferidos, prevenindo assim – pelo menos por agora – uma nova invalidação do regime que regula estas transferências, como ocorreu com os antigos Privacy Shield e Safe Harbour.

Em qualquer caso, e tal como o TGUE indica no seu comunicado de imprensa sobre o assunto, a Comissão Europeia deve monitorizar o quadro jurídico das transferências de dados para os Estados Unidos, de modo a que, caso haja desenvolvimentos ou novos elementos que afetem as garantias aplicáveis, a Comissão terá de decidir se modifica ou invalida este regime.

A Audiência Nacional entende que os pedidos de acesso a dados pessoais devem ser submetidos através dos canais estabelecidos para o efeito e não para endereços de correio eletrónico genéricos

O recorrente interpôs recurso contencioso-administrativo para a Audiência Nacional da decisão da Agência Espanhola de Proteção de Dados (AEPD) que indeferiu a sua reclamação por não ter recebido resposta ao seu pedido de acesso a dados pessoais e académicos tratados por uma universidade. O reclamante tinha solicitado o acesso ao seu histórico escolar por correio eletrónico, enviado para um endereço genérico, e, não tendo obtido resposta, recorreu à AEPD. A Agência indeferiu a reclamação, considerando que o interessado não utilizou os canais específicos estabelecidos pela universidade para o exercício dos direitos de proteção de dados, como o e-mail ou o endereço postal indicados na política de privacidade da instituição.

A Audiência Nacional, aplicando o Artigo 15.º do RGPD e o Artigo 13.º da LOPD-gdd, confirmou a decisão da AEPD. O Tribunal entendeu que a universidade não limitou nem obstruiu o direito de acesso, uma vez que o reclamante não demonstrou ter submetido o seu pedido através dos canais expressamente destinados e divulgados pela instituição para o exercício de direitos. A este respeito, o Tribunal declarou que "foi o reclamante quem apresentou o seu pedido fora dos canais estabelecidos, ignorando o estabelecido no site da instituição em causa".

Consequentemente, o recurso é indeferido, a decisão da AEPD de rejeitar o recurso é mantida e o reclamante é condenado no pagamento das custas processuais, com a ressalva de que a sentença é passível de recurso de cassação.

O TJUE analisa a possibilidade de transferência de dados de trabalhadores de uma empresa para a sua empresa-mãe para testar 'software' e declara ilegal a utilização de dados reais sem base legal

O caso diz respeito à utilização indevida de dados pessoais de um trabalhador por uma empresa alemã, parte de um grupo internacional com sede nos EUA.

Em 2017, o grupo implementou um software de recursos humanos baseado na nuvem para fins de teste, estipulando contratualmente que apenas dados limitados (nome, apelido, data de início, local de trabalho e número de telefone profissional) poderiam ser utilizados e proibindo expressamente a utilização de dados reais para fins de administração de pessoal. No entanto, a empresa carregou dados sensíveis do trabalhador na nuvem, incluindo salário, morada, data de nascimento, estado civil, número de segurança social, nacionalidade e número de identificação fiscal, que foram tratados até 2019.

O trabalhador interpôs uma ação no Tribunal do Trabalho, alegando que a utilização de dados reais era desnecessária para efeitos de teste e que o âmbito permitido tinha sido excedido, pedindo uma indemnização por danos não materiais. Tanto o tribunal do trabalho de primeira instância como o tribunal regional indeferiram a ação.

Posteriormente, o Tribunal Federal do Trabalho submeteu uma questão prejudicial ao Tribunal de Justiça da União Europeia (TJUE) sobre a interpretação do Artigo 88.º, n.º 1, do RGPD relativamente à legislação laboral alemã. O TJUE reiterou que as normas nacionais sobre o tratamento de dados no local de trabalho devem cumprir integralmente as condições e limitações do RGPD, em particular os artigos 5.º, 6.º e 9.º.

Finalmente, o tribunal concluiu que a empresa tratava dados pessoais sem base legal, infringindo o artigo 6.º, n.º 1, do RGPD, e atribuiu ao trabalhador uma indemnização de 200 euros pela perda do controlo sobre os seus dados (Artigo 82.º, n.º 1, do RGPD). Além disso, sublinhou que a utilização de dados reais em testes só seria lícita se os dados fictícios fossem insuficientes para o fim pretendido, o que não se verificava neste caso.

Os tribunais admitem o uso de imagens de videovigilância como meio de prova em processos penais

O Tribunal da Relação de Évora no acórdão de 3 de junho de 2025, **Proc. 412/21.6JAFAR.E1**, pronunciou-se sobre a admissibilidade da utilização de imagens captadas por sistema de videovigilância como meio de prova em processo penal. Estava em causa a utilização de gravações obtidas por câmaras instaladas no exterior de uma discoteca, que captaram a prática de um crime. O tribunal entendeu que as imagens não invadiam o núcleo da vida privada do arguido, e tinham sido recolhidas em local público com o objetivo de documentar factos penalmente relevantes, sendo, por isso, admissíveis como meio de prova. A decisão sustenta-se no princípio da justa causa e na inexistência de violação do princípio da proporcionalidade, referindo que a proteção conferida pelo RGPD, embora aplicável, não impõe neste contexto uma exclusão automática da prova.

Um acórdão esclarece que o consentimento do titular de dados não substitui a autorização judicial quando está em causa apresentar provas no âmbito de um processo judicial

O Tribunal da Relação do Porto no acórdão de 30 de abril de 2025, **Proc. 875/24.8PDVNG-A.P1**, analisou a possibilidade da utilização, em processo penal, de dados de localização GPS instalados num veículo automóvel. O caso dizia respeito ao pedido formulado pelo Ministério Público à operadora de telecomunicações responsável, com o objetivo de obter a localização de um veículo furtado. Apesar de o titular do contrato ter consentido na recolha, a operadora recusou a entrega dos dados sem intervenção judicial. O tribunal confirmou a necessidade de autorização do juiz de instrução para a validação do meio de prova e para junção ao processo penal, considerando que a utilização de dados de localização em sede penal pode interferir com direitos fundamentais, exigindo controlo jurisdicional prévio. A decisão clarifica que o consentimento do titular não substitui a exigência de tutela judicial quando esteja em causa a admissibilidade processual dos dados.

Parecer da CNPD sobre a transmissão pela internet de reuniões de órgãos locais

A CNPD emitiu o Parecer n.º 29/2025 sobre a transmissão online das reuniões dos órgãos das autarquias locais, na sequência de pedido da Junta de Freguesia das Avenidas Novas. A CNPD confirma o entendimento já adotado em 2023, considerando que a transmissão em direto (áudio e

vídeo) online destas reuniões não possui enquadramento legal no regime jurídico das autarquias locais nem no princípio da transparência previsto no RGPD.

Sublinha que embora a publicidade das reuniões se encontre legalmente prevista, não implica a sua difusão por meios digitais. A transmissão em direto, ao expor sistematicamente imagens, vozes e opiniões de participantes, pode violar o princípio da minimização e representar uma alteração da finalidade da recolha de dados. Por esta razão, a CNPD considera que este tipo de difusão configura um tratamento adicional que exige uma nova base legal e, em regra, uma avaliação de impacto, realçando a necessidade de cumprimento escrupuloso do artigo 13.º do RGPD, de forma a que os titulares dos dados sejam total e claramente informados deste tratamento.

O parecer admite que a gravação e disponibilização posterior das reuniões pode ser realizada apenas com base no consentimento dos intervenientes, nos termos do artigo 6.º, n.º 1, alínea a), do RGPD, desde que cumpridos plenamente os requisitos aplicáveis ao consentimento e previstos no RGPD. A este respeito, a CNPD tinha já salientado que o referido consentimento deve ser recolhido não apenas em relação àqueles que, no exercício das suas funções ou no exercício do direito de participação, façam declarações durante as reuniões, como também em relação aos que exercem o mesmo direito de participação através da mera presença ou assistência naquelas. A CNPD sublinha, por fim, a necessidade de distinguir entre titulares de cargos públicos, cujos dados podem estar sujeitos a menor expectativa de privacidade, e cidadãos intervenientes, cujos dados exigem maior proteção.

Em 2023, a CNPD tinha já publicado as **Orientações relativas à transmissão na internet das reuniões de órgãos autárquicos**, nas quais se baseia fundamentalmente o Parecer emitido.

5. Atualidade

O Regulamento de Dados da União Europeia ('Data Act') é aplicável a partir de 12 de setembro de 2025

Desde 12 de setembro de 2025, é aplicável em toda a União o Regulamento (UE) 2023/2854, conhecido como *Data Act*, uma legislação fundamental para promover um mercado de dados mais aberto e competitivo na Europa. O regulamento entrou em vigor em dezembro de 2023, mas a sua aplicação geral começa agora, com disposições que afetam os fabricantes de dispositivos conectados, os prestadores de serviços na nuvem e todas as entidades que gerem dados gerados pela Internet das Coisas (IoT).

O *Data Act* estabelece direitos específicos para os utilizadores de produtos e serviços conectados, garantindo-lhes o acesso e a capacidade de reutilizar os dados gerados pelos seus dispositivos. Além disso, impõe obrigações para a troca equitativa de dados entre empresas (B2B), permite o acesso restrito por parte de organismos públicos em casos de emergência ou de excecional interesse público e promove a interoperabilidade e a portabilidade nos serviços *cloud*, com uma redução progressiva dos custos de mudança de fornecedor.

O *Data Act* estabelece um calendário de implementação faseado. Desde 12 de setembro de 2025 que estão em vigor as obrigações gerais do regulamento, como as relativas à transparência no acesso e partilha de dados e as regras contratuais para evitar cláusulas abusivas nos contratos B2B. Posteriormente, a partir de setembro de 2026, serão ativados requisitos técnicos mais específicos, como a obrigatoriedade de que os produtos e serviços conectados sejam concebidos para permitir o acesso direto aos dados por parte dos utilizadores. Finalmente, em 2027, certas disposições serão também alargadas aos contratos de longo prazo já existentes.

O *Data Act* é sempre aplicado em coordenação com o Regulamento Geral de Proteção de Dados, cuja primazia é expressamente enfatizada, garantindo um equilíbrio entre a economia de dados, a inovação tecnológica e a proteção da privacidade.

Pode consultar aqui o artigo "O *Data Act* entra em cena: peças de um xadrez normativo que nenhuma empresa pode ignorar", de Begoña González Otero, of counsel de Propriedade Industrial e Intelectual da Garrigues e especialista em direito digital.

A Comissão Europeia publica uma resolução em que refere que a Apple e a Meta infringiram o Regulamento dos Mercados Digitais e aplica-lhes coimas de 500 milhões de euros e 200 milhões de euros, respetivamente

A Comissão emitiu uma resolução que sanciona a Meta e a Apple por incumprimento do *Digital Markets Act* (DMA).

No caso da Apple, a Comissão determinou que a empresa violou a obrigação de permitir que os programadores de aplicações informem gratuitamente os utilizadores sobre ofertas alternativas fora da *App Store*, assim como a possibilidade de os redirecionar para essas ofertas. Foi aplicada uma coima de 500 milhões de euros, com a obrigação de remover todas as restrições técnicas e comerciais ao redirecionamento e de se abster de perpetuar esta conduta no futuro.

Por outro lado, em relação à Meta — em que a decisão se aproxima mais da área da proteção de dados pessoais — foi imposta uma penalização por incumprimento do Artigo 5.º, n.º 2, alíneas a), b) e c) do *Digital Markets Act* pela utilização do sistema "*pay or okay*" em relação ao tratamento de dados para publicidade personalizada. De referir que a empresa introduziu um novo modelo que está a ser analisado pela Comissão para determinar a sua legalidade. Por fim, a Comissão decidiu sancionar a Meta com uma coima de 200 milhões de euros.

O CEPD publica a Declaração de Helsínquia e anuncia novas medidas para simplificar e reforçar a implementação do RGPD

O Comité Europeu para a Proteção de Dados (CEPD) publicou a **Declaração de Helsínquia sobre maior clareza, apoio e envolvimento**, anunciando uma série de iniciativas destinadas a facilitar a aplicação prática do RGPD e a reforçar a coerência na sua implementação em toda a União Europeia.

Entre as principais medidas anunciadas, destacam-se:

- **Simplificação de procedimentos**: desenvolvimento de modelos de referência para as organizações, incluindo um modelo comum para notificar as autoridades de proteção de dados sobre violações de dados pessoais.

- **Reforço da coerência**: compilação e partilha de posições adotadas pelas autoridades nacionais, decisões administrativas e decisões judiciais, com o objetivo de produzir publicações que sirvam de "jurisprudência" de referência para as organizações.

- **Coordenação inter-regulatória**: desenvolvimento de orientações conjuntas com outros organismos reguladores europeus para promover uma aplicação consistente em diferentes quadros regulamentares que afetam as organizações.

Com esta declaração, o CEPD procura responder às exigências de maior clareza regulamentar e apoio prático às organizações, promovendo simultaneamente um quadro uniforme para o cumprimento do RGPD em toda a União.

Chile: A Comissão de Implementação da nova Lei de Proteção de Dados publica três relatórios

A Comissão Consultiva Ministerial para a Implementação da Lei de Proteção de Dados Pessoais apresentou este ano três relatórios com várias recomendações para a implementação desta nova regulamentação no país. O primeiro relatório aborda a Agência de Proteção de Dados Pessoais (APDP), recomendando que a sua operacionalidade seja antecipada para junho de 2026, e recomendando também o reforço da sua estrutura e orçamento para garantir a proteção eficaz dos dados pessoais.

O segundo relatório centra as suas recomendações na entrada do Chile nas cadeias de valor digitais, fomentando a inovação e garantindo a confiança dos investidores e parceiros comerciais. Estas recomendações incluem a aprovação de normas corporativas vinculativas apresentadas pelas empresas e cláusulas contratuais-tipo, bem como a exploração dos fluxos internacionais de transferência de dados com os parceiros comerciais da APEC. Considera ainda a declaração dos países que oferecem níveis adequados de proteção de dados e recomenda o início do processo de reconhecimento do Chile como um país adequado e o processo de adesão à Convenção 108+ do Conselho da Europa.

O terceiro relatório dirige as suas recomendações ao setor público e propõe que a Secretaria do Governo Digital emita uma circular com orientações e guias técnicos para assegurar a implementação coordenada da Lei de Proteção de Dados Pessoais em todos os órgãos da Administração Pública. Entre as medidas prioritárias encontram-se a nomeação de encarregados da proteção de dados, a criação de comissões internas de implementação, a adoção de políticas e procedimentos de tratamento de dados para o exercício dos direitos ARCO (Acesso, Retificação, Cancelamento e Oposição), e a implementação de medidas de segurança e planos de formação, entre outras.

O CEPD adota as diretrizes 3/2025 sobre a interação entre o DSA e o RGPD

O Comité Europeu para a Proteção de Dados (CEPD) adotou em 12 de setembro de 2025 as suas Diretrizes 3/2025 para esclarecer como se coordenam o *Digital Services Act* (DSA) e o RGPD.

O CEPD sublinha que o DSA prossegue objetivos distintos e complementares, não se sobrepõe ao RGPD, nem cria uma base jurídica independente para o tratamento de dados pessoais: quando o cumprimento do DSA envolva o tratamento de dados, os prestadores devem identificar uma base do Artigo 6.º do RGPD e respeitar os princípios da minimização de dados, da limitação da finalidade e da proporcionalidade.

As diretrizes abordam em detalhe áreas sensíveis. Nos sistemas de "*notice and action*" e nas reclamações internas (artigos 16.º, 17.º, 20.º e 23.º do DSA), apenas devem ser tratados os dados estritamente necessários e, quando adequado, a identidade do notificante só deve ser divulgada se for absolutamente necessário, com as devidas salvaguardas. Além disso, qualquer decisão automatizada deve respeitar as restrições do RGPD, incluindo as relativas a categorias especiais de dados. No que diz respeito aos padrões obscuros (*dark patterns*), o CEPD reitera que o artigo 25.º do FDA deve ser lido em conjunto com o RGPD: o consentimento e outras escolhas relativas ao tratamento de dados pessoais não podem ser manipulados. A publicidade baseada em categorias especiais de dados é proibida, mesmo que, em teoria, exista uma base jurídica ou uma exceção ao abrigo do Artigo 9.º, n.º 2, do RGPD.

Para motores de busca e plataformas de grande dimensão (VLOPs/VLOSEs), o CEPD enfatiza a gestão de riscos sistémicos (DSA), acompanhada da proteção de dados desde a conceção e por defeito e, quando apropriado, avaliações de impacto sobre a proteção de dados (AIPD) ao abrigo do RGPD. Recomenda que se evitem mecanismos de verificação da idade que identifiquem inequivocamente os utilizadores ou armazenem permanentemente a sua idade; e apela a uma estreita coordenação entre os *digital services coordinators*, a Comissão e as autoridades de proteção de dados, bem como à sua participação no desenvolvimento de códigos de conduta para o DSA, de forma a garantir a sua coerência com os previstos no Artigo 40.º do RGPD.

Relatório Anual da AEPD de 2024: principais resultados e tendências

A Agência Espanhola de Proteção de Dados (AEPD) publicou o seu Relatório Anual de 2024 que apresenta um panorama misto: embora o número de reclamações resolvidas

tenha diminuído, tanto o montante total das coimas como a pressão sancionatória em sectores-chave aumentaram. Em 2024, foram aplicadas 281 coimas (-23% face a 2023), totalizando 35,6 milhões de euros (+19%). Os setores com as coimas mais elevadas foram a energia/água, as instituições financeiras, os serviços de internet, as telecomunicações e a contratação fraudulenta. A coima mais elevada do ano, de 5 milhões de euros, foi aplicada por falta de transparência na informação prestada aos utilizadores, ausência de base legal válida para determinadas atividades de tratamento de dados e deficiências no cumprimento dos princípios da licitude e da lealdade na utilização dos dados pessoais.

No âmbito das violações de dados pessoais, a Agência recebeu 2933 notificações (+46% face ao ano anterior). 84% vieram do setor privado e 16% do setor público, afetando potencialmente mais de 100 milhões de pessoas. Os processos relacionados com violações resultaram em mais de 13 milhões de euros em coimas.

Em matéria de procedimentos, a AEPD resolveu 18.132 reclamações em 2024 (-11% em relação ao ano anterior). O papel do Encarregado da Proteção de Dados (DPO) continuou a consolidar-se: foram certificados 206 DPO em 2024 (total acumulado de 1306), tendo sido notificados 11.227 DPO, que abrangem 119.803 responsáveis pelo tratamento de dados. Destes, 11,63% já possuem certificação oficial. Por fim, os serviços ao cidadão apresentaram um forte crescimento, com 98.162 consultas atendidas (+42,5%), refletindo uma maior procura de orientação sobre proteção de dados.

A Comissão Europeia publicou um relatório sobre a implementação da Estratégia Global de Saúde da UE

Na sequência da entrada em vigor do Regulamento (UE) 2025/327, que estabelece o Espaço Europeu de Dados de Saúde (EEDS), a Comissão Europeia publicou no dia 10 de julho de 2025 um relatório relativo à execução da estratégia da EU para a saúde a nível mundial (COM(2025) 392).

Este relatório apresenta as principais ações tomadas e o progresso realizado em matérias prioritárias para a melhoria da saúde global. Em particular, destaca o progresso conseguido na execução da Estratégia Global de Saúde, focada em três grandes prioridades: promoção da saúde; reforço dos sistemas de saúde; e proteção contra ameaças para a saúde.

O relatório é dirigido ao Parlamento Europeu, Conselho, Comité Económico e Social Europeu e Comité das Regiões, e presta informações sobre as ações realizadas, resultados alcançados e desafios na execução da estratégia de saúde global da UE.

Em destaque, o relatório salienta o reforço da governação dos dados de saúde. A este respeito, é referido que um dos objetivos da estratégia da UE para a saúde a nível mundial consiste em tirar partido do facto de a UE ser pioneira na regulamentação dos dados de saúde e dos certificados digitais, utilizando o armazenamento em nuvem para a partilha de dados, a proteção de dados e a privacidade. É assim, um dos objetivos, que a UE aproveite o potencial dos dados de saúde fora da UE, em consonância com os princípios do Espaço Europeu de Dados de Saúde, que visam promover uma governação mais forte dos dados de saúde e uma maior interoperabilidade. Um dos exemplos práticos que contribui para o avanço no cumprimento deste objetivo diz respeito ao projeto lançado pelo Gabinete Regional da OMS para a Europa e a Comissão Europeia, no âmbito do Programa UE pela Saúde, para reforçar os sistemas de informação sobre saúde e impulsionar a governação e a interoperabilidade dos dados de saúde em 53 países da região europeia da OMS. Este projeto quadrienal visa melhorar a utilização e a reutilização dos dados de saúde pelos prestadores de cuidados de saúde, decisores políticos e doentes, bem como melhorar a qualidade e a interoperabilidade dos sistemas de informação sobre saúde.

A estratégia destaca esforços direcionados para prioridades críticas na saúde a nível mundial, detalhando avanços alcançados e medidas em curso pela UE neste domínio. Designadamente, em conjunto com este relatório, foi também publicado o respetivo Anexo que apresenta uma lista não exaustiva de ações-chave para a execução da estratégia global da saúde.

A Comissão continuará empenhada em acompanhar a concretização do Espaço Europeu de Dados de Saúde e terá até março de 2027 para adotar vários atos de execução essenciais, que estabeleçam regras pormenorizadas para a operacionalização do Regulamento (UE) 2025/327.

Publicado um relatório conjunto da Agência Espanhola de Proteção de Dados (AEPD) e da Autoridade Europeia para a Proteção de Dados (EDPS) sobre as implicações para a privacidade da utilização da aprendizagem federada em inteligência artificial

A AEPD e a EDPS publicaram um relatório conjunto sobre a aprendizagem federada, uma técnica para treinar modelos de inteligência artificial. Esta técnica envolve o treino de modelos localmente em cada dispositivo e a partilha apenas dos resultados, sem enviar os dados originais para um servidor central, reduzindo assim o risco de violações de dados e acesso não autorizado. O relatório destaca as aplicações no setor da saúde, assistentes de voz e veículos autónomos.

O relatório reafirma que a aprendizagem federada está alinhada com princípios como a minimização de dados e a limitação da finalidade, bem como o reforço da responsabilização proativa e da auditabilidade. No entanto, alerta que os parâmetros trocados não devem ser considerados anónimos sem uma análise técnica e jurídica, pois podem permitir inferências sobre dados sensíveis. Realça ainda a necessidade de implementar medidas de segurança em todo o ecossistema, garantir a qualidade e a ausência de enviesamento nos dados distribuídos e proteger o sistema contra ataques que explorem o elo mais fraco.

O Comité Europeu de Proteção de Dados (CEPD) publica a versão final das Diretrizes 2/2024 sobre o Artigo 48.º do RGPD

Após a publicação provisória das diretrizes sobre o Artigo 48.º do RGPD relativas à transferência de dados para as autoridades de países terceiros, foi publicada a versão definitiva com algumas alterações em relação à primeira versão.

As referidas diretrizes, conforme se explicou na newsletter do mês de abril, centram-se nos pedidos de cooperação direta entre uma autoridade pública de um país terceiro e uma entidade privada na UE, enfatizando a necessidade de essas transferências se basearem num fundamento legítimo e num dos mecanismos previstos no RGPD para transferências internacionais de dados. A versão definitiva inclui alguns esclarecimentos, dos quais destacaremos os mais relevantes.

Estas diretrizes não se aplicam se o pedido de transferência tiver origem numa filial ou empresa-mãe do grupo fora do EEE, mesmo que seja apoiado por um pedido de uma autoridade localizada nesse país fora do EEE. Além disso, reforça a ideia de que, se o pedido for feito pela autoridade a um subcontratante para o tratamento de dados, este deve informar o responsável pelo tratamento dos dados e seguir as suas instruções, desde que a lei não o proíba com base num interesse público relevante. Por último, acrescenta ainda que os acordos internacionais em que se baseia a transferência devem permitir às autoridades solicitar informações a entidades privadas e que não se trate de uma mera cooperação entre autoridades públicas. Em caso de dúvida quanto à existência e ao conteúdo de um acordo internacional, o CEPD indica que se devem consultar as autoridades nacionais (Ministério da Justiça e Ministério dos Negócios Estrangeiros, entre outras).

O Conselho e o Parlamento Europeu chegam a acordo para melhorar o cumprimento transfronteiriço do RGPD em benefício dos cidadãos

O Conselho e o Parlamento Europeu chegaram a um acordo provisório sobre um novo ato jurídico (que se prevê vir a assumir a forma de um regulamento) para simplificar e harmonizar os procedimentos administrativos transfronteiriços em matéria de proteção de dados, aumentando a cooperação entre as autoridades de supervisão e, assim, melhorando a eficiência da implementação do RGPD.

Neste sentido, o novo regulamento reconhece vários aspetos, incluindo a flexibilização dos requisitos para que os reclamantes sejam ouvidos nos procedimentos de reclamação e a uniformização dos prazos para a conclusão das investigações (15 meses, prorrogáveispor mais 12 meses, exceto para investigações simplificadas, que devem estar concluídas em 12 meses). Da mesma forma, foi acordado um mecanismo de resolução antecipada, permitindo às autoridades de proteção de dados resolver um caso antes de envolver outras autoridades estrangeiras.

Além disso, está incluída uma medida que exige que a autoridade líder envie um resumo das principais questões às suas congéneres da União Europeia. Por último, mantém-se uma proposta do Conselho relativa a um procedimento de cooperação simplificado, que consiste na possibilidade de não aplicar a normativa adicional para os procedimentos transfronteiriços quando uma questão não suscitar uma complexidade excessiva, reduzindo assim a carga administrativo para as autoridades.

A AEPD analisa se é obrigatório um sistema de inteligência artificial utilizado em comunicações comerciais automatizadas compreender e implementar políticas de privacidade

A Agência Espanhola de Proteção de Dados (AEPD) está a examinar um caso em que uma empresa envia comunicações comerciais automatizadas através de um sistema de inteligência artificial que utiliza mensagens instantâneas. O destinatário das mensagens alega não ter dado o seu consentimento e estar inscrito na Lista Robinson e solicita que as mensagens sejam interrompidas. No entanto, a empresa tinha estabelecido um procedimento claro e gratuito para se opor ao tratamento de dados para fins promocionais, que consistia em responder com a palavra “baja” ("cancelar"). O sistema de IA apenas reconheceu esta palavra e não foi programado para interpretar outras formas de oposição. Apesar dos repetidos pedidos do destinatário para cancelar a subscrição, o sistema não processou o pedido porque não utilizou o termo exato.

A AEPD destaca vários pontos-chave:

i. Procedimento de oposição claro e gratuito: a empresa ofereceu um método simples para se opor ao tratamento de dados (enviar “baja”), cumprindo assim as normas de proteção de dados.

ii. Limitações do sistema de IA: a Agência considera que, embora fosse desejável que os sistemas de IA fossem capazes de interpretar qualquer formulação humana de oposição, não é legalmente exigido que estejam preparados para o fazer. Não se pode exigir que um sistema automatizado compreenda todas as formas possíveis pelas quais uma pessoa pode exercer os seus direitos.

iii. Informação sobre a utilização de IA: a AEPD recorda que, a partir de agosto de 2026, será obrigatório informar expressamente os utilizadores de que estão a interagir com um sistema de IA,

embora atualmente apenas recomende esta prática.

iv. Disponibilidade de outros canais: sublinha-se que a pessoa poderia exercer os seus direitos através de outros meios, como o e-mail ou o site, e que existia apoio humano disponível para responder a estes pedidos.

Em conclusão, a AEPD entende que a empresa cumpriu a obrigação de oferecer um canal claro e gratuito para o exercício do direito de oposição e que o sistema de IA não é obrigado a interpretar todas as mensagens. Além disso, a existência de canais alternativos de contacto com agentes humanos reforça a posição da empresa em relação ao cumprimento da legislação.

A AEPD responde à consulta prévia sobre a utilização de biometria para o controlo de acessos em instalações da Guardia Civil

A Agência Espanhola de Proteção de Dados (AEPD) emitiu uma resposta a uma consulta prévia realizada com base no Artigo 36.º do RGPD, relativa à implementação de um sistema de controlo de acessos biométricos nas instalações de uma entidade de segurança pública.

O sistema proposto não gera uma base de dados centralizada, mas mantém o modelo biométrico na posse do utilizador, reduzindo assim os riscos de tratamento em massa. A finalidade do tratamento é a identificação e o controlo de acessos de pessoas singulares, veículos e residentes em instalações sensíveis, com base em diversas normas, como a Lei Orgânica 7/2021, a Lei Orgânica 2/1986 e oRGPD.

A AEPD analisa a legitimidade do tratamento, salientando que os dados biométricos são categorias especiais que requerem garantias reforçadas. Distingue-se entre identificação e autenticação, sendo esta última menos intrusiva e mais proporcional em contextos controlados. O sistema integra medidas técnicas avançadas, como a geração local de identificadores irreversíveis, o controlo exclusivo pelo titular dos dados, a ausência de armazenamento centralizado e a estrita limitação para fins de autenticação. Estas características minimizam o impacto nos direitos fundamentais.

A AEPD conclui que o tratamento biométrico proposto cumpre os requisitos de legalidade, necessidade e proporcionalidade, e que não existem alternativas igualmente eficazes com menor impacto. Contudo, recomenda uma avaliação diferenciada em áreas menos críticas, bem como a possibilidade de oferecer alternativas não biométricas em determinados casos. Por fim, sublinha a importância da realização de avaliações de impacto periódicas, da garantia do cumprimento do Quadro Nacional de Segurança e da manutenção da proteção de dados sob o controlo exclusivo do titular, prevenindo a sua utilização indevida ou o acesso por terceiros.

Comissão Europeia publica um guia sobre as obrigações dos modelos de IA de finalidade geral

A Comissão Europeia publicou diretrizes interpretativas sobre o âmbito das obrigações aplicáveisaos fornecedores de modelos de inteligência artificial de finalidade geral (GPAI) ao abrigo do Regulamento (UE) 2024/1689 (AI Act), em vigor a partir de 2 de agosto de 2025.

As diretrizes da Comissão Europeia sobre o Regulamento de Inteligência Artificial (AI Act) clarificam as obrigações que os fornecedores de modelos de IA de finalidade geral devem cumprir, especialmente os que apresentem risco sistémico. Estabelecem critérios técnicos (como a contagem de treino em FLOP) para identificar estes modelos, detalham as obrigações relativas à transparência, documentação, conformidade com os direitos de autor e avaliação de riscos, e preveem isenções para modelos de *open-source* em condições estritas.

Além disso, regulam a supervisão pelo Gabinete de IA, os procedimentos de notificação e classificação e o regime de

transição até à implementação integral do regime sancionatório em agosto de 2026.

O CEPD emite uma declaração sobre as cláusulas contratuais-tipo não vinculativas da Lei de Proteção de Dados

O Comité Europeu de Proteção de Dados (CEPD) emitiu uma declaração sobre as cláusulas contratuais modelo (MCT) propostas pela Comissão Europeia para facilitar a troca de dados ao abrigo do Artigo 41.º do *Data Act*.

O CEPD alerta que estas cláusulas, embora não sejam vinculativas, devem estar em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) no que diz respeito ao tratamento de dados pessoais. Entre as suas observações, destaca a necessidade de distinguir claramente entre dados pessoais e não pessoais, melhorar a estrutura e as definições das MCT e garantir que as cláusulas contratuais não prevalecem sobre os regulamentos de proteção de dados em caso de conflito.

O documento observa ainda que o cumprimento das CTM não garante, por si só, a conformidade com o RGPD, e que podem ser necessárias medidas adicionais, como cláusulas contratuais-tipo para transferências internacionais. Recomenda ainda que se considere a vulnerabilidade do consumidor e que se evitem cláusulas penais desproporcionais.

O CEPD mantém-se disponível para continuar a colaborar no aperfeiçoamento destes instrumentos contratuais.

O CEPD está a contribuir para a consulta pública da Autoridade Bancária Europeia (EBA) sobre o projeto de normas técnicas de regulação (RTS) para a prevenção do branqueamento de capitais e do financiamento do terrorismo (AML/CFT)

O CEPD refere que, uma vez que as entidades sujeitas às obrigações de AML/CFT podem ser pessoas singulares, implicando o tratamento de dados pessoais, as RTS devem incluir uma referência à aplicabilidade do RGPD.

Apresenta ainda diversas sugestões de modificações às RTS propostas, tais como:

i. Incluir uma referência explícita à obrigação de implementar medidas técnicas e organizacionais adequadas, conforme exigido pelo Artigo 32.º do RGPD.

ii. No que diz respeito à verificação remota da identidade, o tratamento de dados pessoais não deve ser baseado no consentimento, uma vez que o fornecimento desta informação não é opcional para o cliente. Por conseguinte, a AEPD sugere que a base jurídica seja o cumprimento de uma obrigação legal (Artigo 6.º, n.º 1, alínea c) do RGPD).

iii. Convém esclarecer que as informações armazenadas devem ser atualizadas e retificadas sem demora injustificada.

iv. Deve ser assegurado que o princípio da minimização de dados é respeitado na recolha de dados pessoais de terceiros em casos de suspeita de atividade criminosa.

A AEPD e a Autoridade de Proteção de Dados do Brasil alargam a sua colaboração institucional

No âmbito da *Global Privacy Assembly* (GPA), realizada em Seul, o Presidente da Agência

Espanhola de Proteção de Dados (Lorenzo Cotino) e o Diretor-Presidente da Autoridade Nacional de Proteção de Dados do Brasil (Waldemar Gonçalves) assinaram a renovação do Memorando de Entendimento (MOU) entre as duas instituições. Este acordo reforça a colaboração institucional e estabelece um quadro para o desenvolvimento de ações conjuntas com o objetivo de promover e implementar a proteção de dados pessoais.

O Memorando de Entendimento inclui o intercâmbio de conhecimentos técnicos, a cooperação em investigações, estudos e análises, bem como o desenvolvimento de guias e ferramentas para facilitar o cumprimento das normas regulamentares. Além disso, prevê o desenvolvimento de iniciativas conjuntas, especialmente no âmbito de programas e projetos internacionais.

Na esfera ibero-americana, destaca-se o trabalho conjunto no âmbito da Rede Ibero-Americana de Proteção de Dados. Este fórum é atualmente presidido pela ANPD (Agência Nacional de Proteção de Dados) e tem como secretariado permanente a Agência Espanhola. Entre as conquistas recentes, destaca-se a aprovação das "Normas Ibero-Americanas de Proteção de Dados", que promovem a adoção de mecanismos para a troca de boas práticas e experiências entre os países da região.

Este acordo consolida a cooperação internacional e a liderança de ambas as autoridades na proteção de dados pessoais a nível global e ibero-americano.

Investigadores do 'Joint Research Centre' da Comissão Europeia publicam um artigo sobre 'AI Benchmarks'

No artigo analisam-se os problemas e as limitações dos *benchmarks* ou indicadores de referência em inteligência artificial (IA), que se tornaram ferramentas essenciais para avaliar o desempenho, as capacidades e os riscos dos sistemas de IA, e são cada vez mais relevantes tanto para a investigação como para a regulamentação, especialmente no contexto da implementação do *European AI Act*. Neste sentido, o estudo parte da premissa de que, embora os *benchmarks* permitam a comparação de modelos e a medição do progresso, a sua utilização generalizada tem levantado preocupações sobre a sua adequação para avaliar aspetos sensíveis como a segurança, o impacto social e os riscos sistémicos da IA.

O artigo conclui que os *benchmarks* atuais, na sua maioria quantitativos e orientados para o desempenho, são insuficientes para fornecer as garantias de segurança e fiabilidade exigidas pelos legisladores e pela sociedade. Assim sendo, os autores recomendam que seja exigida maior transparência e documentação na criação e utilização de *benchmarks*, se promova a diversidade e a inclusão na sua conceção, se desenvolvam *benchmarks* dinâmicos e multimodais que reflitam melhor os riscos e capacidades reais dos sistemas de IA e se estabeleçam protocolos rigorosos de validação e atualização.

Além disso, defendem a avaliação não só do desempenho, mas também dos erros, vulnerabilidades e consequências não intencionais dos modelos, bem como a criação de mecanismos para avaliar a fiabilidade dos próprios *benchmarks*, para além da sua popularidade ou número de citações.

O 'Information Commissioner's Office' (ICO) do Reino Unido publica um artigo sobre como garantir a anonimização eficaz dos dados pessoais

O artigo fornece orientações para a anonimização eficaz de dados pessoais, oferecendo uma abordagem prática e estratégica para garantir que este processo é realizado de forma eficaz, permitindo às organizações tratar dados sem comprometer a privacidade do utilizador.

Para avaliar se um conjunto de dados foi anonimizado de forma eficaz, o ICO propõe a aplicação do chamado *"motivated intruder test"*. Este teste analisa se uma pessoa com motivação, conhecimento e recursos razoáveis poderia identificar um utilizador utilizando os dados anonimizados em conjunto com informações publicamente disponíveis. Se existir uma probabilidade significativa de identificação, os dados não podem ser considerados anónimos.

Além disso, o guia sublinha que a anonimização deve ser eficaz não só para o responsável pelo tratamento de dados, mas também para qualquer terceiro que tenha acesso aos dados. Da mesma forma, o ICO recomenda que as organizações adotem uma abordagem estratégica e técnica, propondo que as avaliações de impacto sobre a proteção de dados (AIPD) sejam realizadas quando necessário e que as decisões e medidas tomadas sejam cuidadosamente documentadas. O guia apresenta medidas práticas para identificar riscos, aplicar técnicas de anonimização adequadas e estabelecer controlos que reforcem a proteção da informação.

Por fim, o artigo conclui destacando os inúmeros benefícios da implementação das medidas descritas, que permitem a partilha e reutilização de dados com menos restrições legais, promovem a inovação responsável e melhoram a transparência para os titulares dos dados. Além disso, reduz a carga regulatória ao excluir os dados anonimizados do âmbito do RGPD do Reino Unido, o que, segundo o ICO, pode facilitar projetos de análise, investigação e desenvolvimento tecnológico.

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

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

Adrián León
Associado - Alicante
adrian.leon@garrigues.com

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

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

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

Manuel Liberal Jerónimo
Sócio · Lisboa e Porto
manuel.liberal.jeronimo@garrigues.com

Sebastián Hassi
Associado principal · Santiago do Chile
sebastian.hassi@garrigues.com

Antonio Durán
Associado - Málaga
antonio.duran@garrigues.com

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

Laia Llambric
Associada - Bilbau
laia.llambrich@garrigues.com

Matilde Bettencourt
Associada · Lisboa
matilde.bettencourt@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

Siga-nos em:

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.