GARRIGUES

Newsletter Economia de Dados, Privacidade e Cibersegurança

Junho de 2025

Índice

1. A Comissão Europeia propõe alterações ao RGPD: leitura crítica e propostas práticas

A Comissão Europeia apresentou uma proposta de alteração do RGPD com o objetivo de reduzir encargos burocráticos para PME, ampliando as exceções à obrigação de manter um Registo de Atividades do Tratamento (RAT) como principal medida. Embora a intenção seja positiva, o enfoque escolhido foi criticado por ignorar a essência da conformidade normativa. Analisamos o que isto implica (não necessariamente uma melhoria para as PME) e propomos algumas alternativas de melhoria para facilitar o cumprimento do RGPD.

Alejandro Padín Vidal

A Comissão Europeia publicou recentemente uma proposta de regulamento destinado a simplificar determinadas obrigações que afetam micro, pequenas e médias empresas. Entre as medidas apresentadas neste documento está uma proposta de alteração ao Regulamento Geral sobre a Proteção de Dados (RGPD). O espírito subjacente a esta proposta é, essencialmente, flexibilizar algumas das obrigações de conformidade do RGPD, com o alegado objetivo de ajudar as pequenas e médias empresas a cumprir sem encargos burocráticos excessivos, procurando assim obter poupanças de custos e maior eficiência da atividade empresarial.

Embora o propósito e a intenção sejam altamente louváveis, o conteúdo das propostas pode não atingir o objetivo ao concentrar-se em algumas questões que estão longe de ser o problema que as PME enfrentam para cumprir o RGPD.

Neste artigo, explicamos isto com exemplos concretos e propomos algumas modificações que seriam úteis para melhorar a situação de cumprimento e adaptá-la à realidade das pequenas e médias empresas.

1. Obrigação de manter um Registo das Atividades de Tratamento e suas exceções

A principal medida incluída na proposta da Comissão diz respeito à obrigação de manter um Registo das Atividades de Tratamento (RAT) estabelecido no artigo 30.º do RGPD. Mais concretamente, a proposta visa alargar o perímetro de exceções aplicáveis a esta obrigação, para que um maior número de empresas decida não manter este registo.

A redação atual do artigo 30.º do RGPD inclui um ponto 5 que contém as seguintes exceções:

"As obrigações a que se referem os n.os 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um

risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.º".

Como se pode ver, o texto obriga qualquer empresa com mais de 250 trabalhadores e também as que tenham menos do que esse número se se verificar alguma destas três circunstâncias: (i) o tratamento implique risco, (ii) não seja ocasional ou (iii) inclua categorias especiais de dados ou antecedentes criminais.

O texto que se pretende substituir o referido n.º 5 do artigo 30.º é o seguinte:

"As obrigações a que se referem os n.os 1 e 2 não se aplicam às empresas ou organizações com menos de 750 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco elevado para os direitos e liberdades do titular dos dados, no sentido do artigo 35.º".

Como se pode observar, para além do aumento do limite do número de trabalhadores, foram eliminadas duas das três circunstâncias em que as pequenas empresas também seriam obrigadas a ter um RAT, a saber, que o tratamento não seja ocasional ou que inclua categorias especiais de dados pessoais.

Refletindo sobre esta proposta de alteração, colocam-se as seguintes questões: não ter um RAT reduz realmente a carga burocrática? Isso representa uma maior facilidade de cumprimento para as pequenas empresas? O nível de cumprimento irá melhorar?

2. Comentário à proposta de alteração

Na nossa opinião, esta proposta de reforma suscita dúvidas por duas razões: em primeiro lugar, porque ignora as origens do atual artigo 30.º, n.º 5 e as razões pelas quais foi incluído um critério numérico no seu texto. Em segundo lugar, porque não tem em conta a essência do que significa o RAT num programa de conformidade com o RGPD e induz em erro as entidades obrigadas sobre a finalidade mais essencial do RGPD.

a. Aumento do número de trabalhadores

Quanto ao primeiro motivo, é necessário recuar à evolução do texto do RGPD durante os quatro anos que levou a sua tramitação nas instituições da UE até à sua aprovação final e publicação no Jornal Oficial da União Europeia (JOUE) como norma obrigatória.

A este respeito, vale a pena recordar que, em algumas das suas versões iniciais, o projeto do RGPD continha vários casos em que determinadas obrigações estavam ligadas a critérios numéricos de uma espécie ou de outra (por exemplo, a obrigação de nomear um Encarregado da Proteção de Dados (DPO) ou representante na União Europeia estava vinculada na versão inicial da proposta do RGPD à entidade responsável que empregasse mais de 250 pessoas; versões posteriores ligavam-na à existência de tratamento que afetasse mais de 5000 titulares de dados; estas barreiras objetivas acabaram por ser eliminadas). Nesta linha de objetivar obrigações, o artigo 30.º estabeleceu a obrigatoriedade de possuir um RAT para as empresas com mais de 250 trabalhadores. Neste caso, ao contrário dos restantes em que foram eliminadas as referências numéricas, manteve-se o critério numérico.

Ao longo do seu percurso pelas instituições europeias, a tramitação do RGPD oscilou entre uma abordagem jurídica baseada sobretudo nos sistemas de codificação napoleónicos, de natureza administrativa (direito continental europeu), e uma abordagem anglo-saxónica (*Common Law*, com uma componente de "*accountability*").

"*Accountability*" é um conceito jurídico que não tem tradução direta para português. Na versão portuguesa do RGPD é traduzido como "responsabilidade", enquanto no Regulamento de Inteligência Artificial é traduzido como "responsabilização". O conteúdo completo da "*accountability*" inclui: (i) a obrigação de cumprir uma obrigação específica, (ii) ser capaz de demonstrar o cumprimento em todos os momentos, e (iii) responsabilização ou responsabilidade em caso de incumprimento de qualquer das duas obrigações acima referidas.

O resultado final deste processo foi uma lei híbrida, que inclui artigos representativos de ambos os sistemas jurídicos. Assim, por exemplo, podemos ver nos artigos 13.º e 14.º (obrigação de informar), no artigo 28.º (conteúdo do contrato com o subcontratante para o tratamento) e no artigo 30.º (RAT) uma representação clara da tradição mais administrativa e, pelo contrário, nos artigos 5.º, n.º 2 (princípio da responsabilidade), artigo 25.º (privacidade desde a conceção e por defeito) ou artigo 32.º (segurança do tratamento) como representações claras do *Common Law*.

A revisão final e o consenso necessários para publicar uma norma aceite por todos estavam longe de ser simples. Sem dúvida, o acordo político alcançado envolveu a eliminação de parâmetros objetivos de conformidade e a sua substituição pela flexibilidade e adaptação a casos concretos, aplicando critérios de análise de risco. Assim, as menções acima referidas (número de trabalhadores ou de tratamentos para EPD, número de trabalhadores ou de titulares de dados afetados para representante da UE, etc.) foram eliminadas e substituídas por obrigações específicas ou por conceitos jurídicos indeterminados, porque se entendeu que a conformidade com a norma não deveria ser determinada com base em limites, mas que o critério mais importante era o risco para os direitos e liberdades dos titulares cujos dados são tratados. Obviamente, o risco do tratamento de dados para as pessoas não depende do número de trabalhadores da entidade que trata os dados ou de qualquer outro critério objetivo. Pode existir uma empresa com 1000 trabalhadores cujo tratamento de dados apresente um risco inferior ao de outra empresa com 25 trabalhadores.

Ora, nesta tarefa final de eliminação de fasquias numéricas, a que se encontra no n.º 5 do artigo 30.º do RGPD só pode ser descrita como um lapso de última hora, uma vez que a conveniência de ter um RAT não tem nada a ver com o número de trabalhadores da entidade. De qualquer modo, mesmo que esta redação não fosse fruto de um lapso, o próprio texto inclui "exceções à exceção" suficientes para que, na prática, o RAT seja obrigatório na grande maioria dos casos, considerando o atual nível elevado de utilização da tecnologia.

Por isso, o aumento do limite de trabalhadores para a obrigação do RAT não é compreensível.

b. Dúvidas sobre a flexibilização geral

O segundo comentário que pode ser feito sobre a abordagem da proposta de alteração à obrigação de ter um RAT está relacionado com a própria essência do que é um RAT e o seu lugar num sistema de cumprimento do RGPD. Não podemos perder de vista que a proposta está a ser apresentada sete anos após a aplicação obrigatória do regulamento, quando já temos experiência e critérios práticos e jurídicos suficientes para compreender verdadeiramente o que é um RAT, a sua importância e o que significa.

Como vimos, para além do critério numérico relativo aos trabalhadores, a proposta elimina a obrigatoriedade de possuir um RAT quando existam tratamentos que envolvam um risco para os direitos e liberdades dos titulares dos dados (substituído por "risco elevado"), quando se trate de tratamentos não ocasionais e quando sejam tratados dados de categorias especiais.

É necessário recordar aqui que o RAT pode ser descrito como a espinha dorsal de um programa de cumprimento do RGPD. E isto porque, mais do que uma mera obrigação formal de elaboração

de um documento, o RAT constitui o inventário detalhado dos tratamentos de dados realizados pelo responsável pelo tratamento. Isto, por sua vez, é essencial para cumprir muitas outras obrigações do RGPD. A mais imediata é a obrigação de informar (artigo 13.º), que obriga o responsável pelo tratamento a comunicar ao titular dos dados todos os elementos importantes que afetam o tratamento. Estes elementos são organizados e detalhados no RAT e, por esse motivo, elaborar uma política de privacidade sem um RAT torna-se uma tarefa complexa e abstrata. O RAT é igualmente importante em relação à verificação das obrigações de conservação de dados, às medidas de segurança, às transferências internacionais, ao controlo e monitorização dos subcontratantes do tratamento e às transferências de dados. Tudo isto se reflete no RAT e serve de guia para o cumprimento do RGPD.

Qualquer pessoa que tenha implementado de forma rigorosa um projeto de cumprimento do RGPD sabe que, sem o RAT, a tarefa se torna significativamente mais complicada. E, por isso, é surpreendente que aumentar o número de casos em que não é necessário um RAT se considere uma "medida de flexibilização". A consequência, longe de ser uma flexibilização e melhoria ou uma redução da burocracia, só poderia ser uma deterioração do nível de cumprimento do RGPD entre as pequenas e médias empresas e uma maior dificuldade em conseguir um programa de conformidade coerente e ordenado. Isto pode criar uma falsa sensação de conformidade para as empresas que beneficiam destas exceções, que terão mais dificuldade em cumprir integralmente o RGPD. E pode aumentar o número de empresas que continuarão a cair, com maior intensidade, nas redes de assessores sem escrúpulos que vendem papel fotocopiado sem conteúdo válido (não sendo necessário um RAT, um programa sem conteúdo pode passar mais facilmente despercebido a alguém sem conhecimentos na área).

3. Propostas de melhoria do RGPD

O RAT não seria, portanto, o ponto em que seria necessário flexibilizar o RGPD. E agora analisamos que medidas seriam realmente úteis para ajudar as pequenas e médias empresas a cumprir a regulamentação e, em última análise, a proteger melhor os direitos e liberdades dos titulares dos dados (que é o verdadeiramente importante).

Com base na experiência dos nove anos desde que o RGPD foi publicado e entrou em vigor em 2016 e dos sete anos de cumprimento obrigatório desde 25 de maio de 2018, existem várias melhorias que poderiam ser feitas, mesmo sem ter de modificar uma única vírgula do RGPD. Alguns exemplos:

- **Promover de forma mais eficiente a publicação de códigos de conduta ou sistemas de certificação.** A proposta de alteração do RGPD pela Comissão inclui também, como segunda e terceira medidas, a inclusão no RGPD de uma referência específica às empresas de média dimensão (*mid-cap*), para além da referência às pequenas e médias empresas que já existia nos artigos que incluem a possibilidade de aprovar códigos de conduta e sistemas de certificação. O que é realmente necessário, no entanto, é incentivar a sua implementação ou promover ativamente a sua criação, por exemplo, publicando modelos de códigos de conduta que as associações do setor possam utilizar como referência.

- **Desenvolver documentação para permitir o cumprimento das avaliações de impacto para as transferências internacionais de dados (DTIA).** Atualmente, é muito frustrante verificar como inúmeras empresas são obrigadas a repetir o mesmo exercício de análise que já foi realizado centenas de vezes por outras empresas, tendo de gastar enormes quantias de dinheiro para obter um relatório que poderia facilmente ter sido elaborado por uma das autoridades públicas competentes. Por exemplo, embora um DTIA exija diversos *inputs* — alguns deles específicos do caso concreto — a realidade é que muitos outros estão relacionadas com a análise do ordenamento jurídico e a aplicação da norma no país

destinatário dos dados. O facto de cada empresa que vai realizar uma transferência internacional com base em cláusulas contratuais-tipo (a grande maioria) para um país específico ter de encomendar um relatório jurídico sobre esse mesmo país representa um ónus burocrático e económico injusto e desproporcional, que poderia ser completamente eliminado com um único relatório elaborado por uma instituição nacional ou europeia para cada país. Escusado será dizer que eliminar o RAT não reduziria este problema real e quotidiano.

- **Auxiliar na interpretação da regulamentação através da implementação de canais de consulta eficazes e úteis por parte das autoridades de controlo.** Concentrar a supervisão num processo de discussão construtivo entre a autoridade e o responsável pelo tratamento de dados, para que o cumprimento possa ir além dos procedimentos sancionadores e para que as empresas não tenham receio de abordar as autoridades e sintam que receberão ajuda, e não silêncio ou evasivas.

- **Apoiar e auxiliar as empresas que sofrem ciberataques a melhorar a sua situação de segurança da informação** porque, na maioria dos casos, senão em todos, apesar de terem investido em cibersegurança, as empresas vêem-se impotentes quando sofrem um ciberataque, e a isso acresce ainda a aplicação de sanções por parte das autoridades de controlo. O regime sancionatório deve ser o "último recurso" na aplicação do RGPD, reservado para casos claros de incumprimento intencional ou reiterado, e não para casos em que as empresas sofrem situações indesejáveis mesmo tendo tentado cumprir o regulamento.

Em síntese, e para concluir, as alterações ao RGPD que visam tornar as empresas mais flexíveis e eficientes sem enfraquecer a proteção de dados pessoais devem ser bem-vindas e incentivadas. Contudo, talvez seja mais simples refletir sobre como esses mesmos objetivos podem ser alcançados sem a necessidade de alterar a regulamentação (que tanto custou a ser aprovada e tanta força tem), abordando os problemas práticos da sua aplicação e facilitando o seu real e efetivo cumprimento pelas entidades obrigadas.

2. Resoluções das autoridades de proteção de dados

A AEPD aplica uma sanção no âmbito de um caso de duplicação fraudulenta de cartão SIM

A Agência Espanhola de Proteção de Dados (AEPD) aplicou uma coima total de 1.200.000 de euros a uma empresa de telecomunicações por duas violações do artigo 6.º do RGPD, relativo às bases legais (200.000 euros) e do artigo 25.º do RGPD, sobre a privacidade desde a conceção e por defeito (1.000.000 euros).

Esta sanção foi imposta no âmbito de um caso de troca de *SIM Swapping*, em que trabalhadores da entidade sancionada cometeram esta fraude no estabelecimento onde trabalhavam. Na decisão é feita referência ao facto de o responsável possuir diversos procedimentos internos relativos ao tratamento de dados pessoais pelo seu pessoal, que incluíam as medidas de implementação necessária. Contudo, a AEPD considera que esta documentação tinha carácter genérico, pois, embora fizesse referência à existência de riscos, estes não eram suficientemente detalhados, nem estabelecia ações específicas a serem tomadas caso estes se concretizassem.

Rejeitando as várias alegações da parte sancionada — que, entre outras, alegou que a AEPD estaria a assumir um critério de responsabilidade objetiva, fruto de uma análise de resultado —, a AEPD conclui que as medidas organizacionais da entidade foram insuficientes, sobretudo tendo em conta que este tipo de fraude é relativamente comum no seu setor e pode ter consequências graves para os titulares dos dados.

Assim, a AEPD acabou por sancionar, para além de pelo tratamento sem fundamento legal nos termos do artigo 6.º do RGPD, por incumprimento do artigo 25.º do RGPD. Trata-se de uma decisão extensa e muito interessante, principalmente pelas apreciações feitas quanto ao nível de diligência que os responsáveispelo tratamento devem adotar quanto ao cumprimento do princípio da privacidade desde a conceção e por defeito.

La Liga, sancionada com um milhão de euros pelo tratamento de dados biométricos

A AEPD aplicou uma sanção de um milhão de euros à Liga Nacional de Futebol Profissional (LNFP) por violação do artigo 35.º do RGPD e ordenou a limitação temporária ou permanente do tratamento de dados biométricos de adeptos em clubes onde os controlos de acesso são efetuados com esta tecnologia, até que seja realizada e aprovada uma Avaliação de Impacto da Proteção de Dados (AIPD) válida.

A sanção deve-se ao facto de a LNFP não ter realizado uma AIPD relativa ao tratamento de dados biométricos para acesso às bancadas

dos estádios de futebol da primeira e segunda divisões, em violação do artigo 35.º do RGPD. Segundo a AEPD, a LNFP era responsável pela realização desta avaliação devido ao seu papel na implementação do sistema de controlo de acesso biométrico.

A AEPD destacou a falta de diligência por parte da LNFP, uma vez que, apesar da informação disponível sobre os riscos associados ao tratamento de dados biométricos, esta entidade impôs um regime obrigatório para os clubes e sociedades anónimas desportivas de tratarem dados biométricos para acesso às bancadas. Além disso, através de uma subsidiária, a LNFP criou os meios técnicos para a implementação do sistema biométrico, influenciando os requisitos de acesso e obrigando os clubes a adotar uma solução técnica específica, tudo isto sem ter realizado a AIPD.

A AEPD sanciona com 600.000 euros uma sociedade mútua por uma violação de segurança que afetou quase 3400 pessoas

A decisão da AEPD no processo EXP202412881 refere-se a uma violação de segurança cometida por uma sociedade mútua colaboradora da Segurança Social que afetou 3395 pessoas cujos dados pessoais, incluindo dados de saúde, foram enviados por engano a 354 entidades não autorizadas.. Este incidente ocorreu durante a utilização de uma plataforma online que permite às empresas parceiras e consultoras receberem ficheiros Excel semanais por e-mail com informações sobre as prestações financeiras dos seus trabalhadores.

A falha técnica que levou à violação ocorreu devido a uma modificação no sistema de notificações automatizadas, que resultou na desativação inadvertida de uma linha de código essencial. Esta linha tinha como função evitar que os ficheiros de destinatários anteriores se acumulassem em remessas subsequentes. Ao não ser executado, os e-mails enviados às entidades continham não só os ficheiros correspondentes, mas também ficheiros que não eram seus, o que originou a exposição massiva de dados pessoais.

A sociedade mútua detetou o erro depois de uma empresa utilizadora a ter alertado e procedeu à correção do código, implementou controlos técnicos e contactou as entidades destinatárias para solicitar a eliminação dos dados, além de ter notificado a AEPD sobre a violação. Além disso, propôs um redesenho do sistema com medidas de segurança melhoradas, rastreabilidade e caducidade automática dos documentos.

A AEPD considerou que a sociedade mútua violou o princípio da integridade e confidencialidade previsto no artigo 5.º, n.º 1, alínea f), do RGPD, ao não implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais. A infração foi classificada como muito grave, de acordo com o artigo 83.º, n.º 5 do RGPD e o artigo 72.º, n.º 1, alínea a) da LOPDGDD. Inicialmente foi proposta uma coima de 1.000.000 de euros, mas foi reduzida para 600.000 euros depois de a sociedade mútua ter reconhecido a responsabilidade e realizado o pagamento voluntário, encerrando assim o procedimento sancionatório.

Rejeitado o direito a ser esquecido sobre informações de acesso público relativas ao emprego público

No Processo N.º EXP202404813, a Agência Espanhola de Proteção de Dados decidiu o procedimento de direitos iniciado por uma reclamação contra uma conhecida empresa de motores de busca online, em que o reclamante solicitava a remoção de vários links que apareciam nos resultados do motor de busca ao introduzir o seu nome e apelido. Alegou que estes links continham informações pessoais desatualizadas e irrelevantes relacionadas com a sua vida profissional e que a sua manutenção violava o artigo 93.º da LOPD-gdd (Lei Espanhola de Proteção de Dados) sobre o direito ao esquecimento.

A entidade reclamada alegou que alguns dos URL já tinham sido objeto de decisão anterior de indeferimento, que outros não apareciam nos resultados da pesquisa e que os restantes se referiam a informação institucional sobre processos de seleção e nomeações para a carreira na função pública. Argumentou que essa informação era de relevância pública e que a sua publicação atendia às obrigações legais de transparência e publicidade ativa.

A AEPD concluiu que os dados pessoais publicados resultam de atos administrativos ligados a processos de seleção regidos pelos princípios do mérito, da capacidade, da igualdade e da publicidade. Considerou que impedir que os motores de busca redirecionassem para esta informação prejudicaria o princípio da publicidade que rege o acesso ao emprego público. Além disso, assinalou que o tempo decorrido desde a publicação (2021 e 2022) não foi suficiente para considerar a informação obsoleta, principalmente quando o reclamante ainda detém a condição de funcionário público de carreira.

A Agência indeferiu, assim, a reclamação, uma vez que não existiam circunstâncias que justificassem que o direito do reclamante prevalecesse sobre o interesse público na manutenção dos links.

Uma empresa foi sancionada por usar o Whatsapp pessoal dos trabalhadores para fins profissionais

A Agência Espanhola de Proteção de Dados decidiu o procedimento sancionatório iniciado contra uma sociedade após uma reclamação de um trabalhador que denunciou o envio reiterado de dados pessoais de clientes para o seu número pessoal de WhatsApp, apesar de ter manifestado expressamente a sua oposição à utilização do seu dispositivo pessoal para o efeito. A empresa alegou que a utilização do WhatsApp era uma prática comum e consensual entre todos os colaboradores e que o reclamante também tinha iniciado comunicações através deste canal.

A AEPD concluiu na sua decisão que a empresa violou o n.º 1 do artigo 6.º do RGPD ao tratar os dados pessoais do reclamante sem base legal, mesmo após o termo da relação de trabalho, e o artigo 32.º do RGPD ao não implementar medidas de segurança adequadas ao enviar dados de clientes para um dispositivo privado cuja configuração não podia controlar. A Agência rejeitou as alegações da empresa, afirmando que nem o costume nem a alegada aceitação tácita justificavam o tratamento, e que o reclamante tinha reiterado a sua recusa em utilizar o seu telemóvel pessoal como instrumento de trabalho.

Foram impostas duas sanções financeiras: uma de 2500 euros por violação do artigo 6.º, n.º 1 do RGPD e outra de 2500 euros por violação do artigo 32.º do RGPD. Além disso, a empresa foi obrigada a demonstrar, no prazo de três meses, que adotou medidas para impedir o contacto com ex-trabalhadores sem base legal e garantir que os dados dos clientes não são enviados para dispositivos pessoais sem cumprir os requisitos do RGPD e da LOPD-gdd.

Sanção dupla no valor total de 3.500.000 euros a uma entidade bancária ao não garantir a segurança dos dados pessoais dos seus clientes

Na decisão PS 00477-2023 foi apresentada uma reclamação por duas pessoas singulares contra um banco depois de se ter descoberto que a mãe de um dos reclamantes tinha acesso não autorizado às informações financeiras das suas contas bancárias. No caso discutido, a mãe constava como autorizada em duas contas detidas exclusivamente por um dos reclamantes, mas as operações bancárias online permitiram-lhe visualizar informações sobre as contas partilhadas e todos os produtos associados, como cartões de crédito, hipotecas e seguros, sem ter autorização para o efeito.

O reclamante apresentou várias reclamações internas à instituição bancária e ao Banco de Espanha sem obter uma solução satisfatória.

O banco reconheceu inicialmente que ocorreu um "incidente técnico" que permitiu à mãe do reclamante aceder a informação não autorizada.

A AEPD determinou que a empresa violou vários artigos do RGPD, incluindo a falta de consentimento explícito e a ausência de medidas adequadas para garantir a segurança dos dados, existindo "negligência no tratamento dos dados". Apesar de ter conhecimento dos factos relatados quando informado pelo reclamante, não foram tomadas as medidas necessárias para impedir a continuidade da violação. Deste modo, considera-se que a parte demandada incorre ainda mais na culpabilidade e ilicitude da sua conduta.

A deliberação conclui com a imposição de uma sanção pecuniária à empresa infratora, bem como a obrigação de adotar medidas corretivas para cumprir as normas de proteção de dados. Os factos constituem uma dupla infração, imputável à parte reclamada, por violação dos artigos 5.º, n.º 1, alínea f) ("princípio da confidencialidade") e 25.º do RGPD ("aplicação de medidas técnicas e organizativas adequadas"). O balanço das circunstâncias consideradas relativamente às infrações cometidas permite à AEPD aplicar uma coima de 500.000 de euros pela primeira infração e outra de 3.000.000 de euros pela segunda.

Aplicada uma coima de 500.000 euros por não comunicar ao responsável pelo tratamento a identidade das entidades que pretendia subcontratar

Em 1 de abril de 2009, o Departamento de Assistência Médica Universal e Saúde Pública da *Generalitat* Valenciana assinou com uma associação que se dedica à prestação de serviços de saúde um contrato relativo à prestação do serviço de assistência médica no Departamento de Saúde de Denia. Este contrato incluía um acordo de tratamento de dados que estipulava a obrigação de o subcontratante informar o responsável pelo tratamento sobre a identidade das empresas a quem pretende subcontratar os serviços abrangidos pelo contrato. Face ao incumprimento desta obrigação, o Departamento apresentou reclamação à AEPD.

Neste caso, não há qualquer prova de que a parte reclamada tenha informado o Departamento antes da formalização dos contratos celebrados com os subcontratantes ulteriores para que, enquanto responsável pelo tratamento dos dados, tivesse tido oportunidade de se opor. Ao decidir sobre o valor da coima administrativa, a AEPD tem em conta a natureza, a gravidade e a duração da violação por não ter comunicado os três contratos celebrados com os subcontratantes ulteriores em 2018, que ainda estão em vigor, e o facto de os dados pessoais afetados pela violação serem dados de saúde, que são considerados categorias especiais de dados. Por todas estas razões, a coima aplicada ascende a 500.000 euros.

Uma entidade bancária condenada por não implementar as medidas adequadas para garantir a confidencialidade dos dados pessoais

Em 28 de outubro de 2022, a AEPD recebeu uma notificação de uma violação de segurança por parte da sucursal espanhola de uma instituição bancária francesa, alegando que um dos subcontratantes ulteriores que essa instituição contratou tinha sofrido um ciberataque de *ransomware*. Na decisão do processo sancionador, a AEPD enfatiza as seguintes questões:

1. Quanto à ausência de legitimidade passiva da sucursal espanhola e à falta de competência territorial da AEPD, considera-se não só a responsabilidade direta da reclamada nos factos, mas também que a agência tem autoridade suficiente para decidir sobre os tratamentos realizados em Espanha.

2. Quanto à alegação de que o banco é vítima de um crime, a AEPD sublinha que a culpabilidade do arguido não pode ser

excluída ou atenuada pelo facto de um terceiro ter participado em atos fraudulentos, uma vez que a sua responsabilidade não decorre da atuação deste, mas sim da sua própria.

3. No que respeita às obrigações previstas tanto no artigo 5.º, n.º 1, alínea f), como no artigo 32.º do RGPD, relativas à necessidade de aplicação de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, que inclui, entre outras, a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e a capacidade de restabelecer o acesso aos dados pessoais de forma célere, a AEPD declara a falta de diligência e adequação das medidas adotadas e implementadas pela entidade no caso concreto, tudo isto tendo em conta os riscos de probabilidade e gravidade variáveispara os direitos e liberdades das pessoas singulares.

4. Em particular, a AEPD concluiu que o acesso de terceiros não teria ocorrido se os dados pessoais tivessem sido encriptados, pseudonimizados ou anonimizados, uma vez que o atacante teria obtido informações ininteligíveis.

Quanto à responsabilidade do responsável pelo tratamento dos dados, a AEPD sublinha que a instituição bancária é responsável pelos dados pessoais, independentemente de qualquer responsabilidade que terceiros alheios à mesma possam ter. Por todos estes motivos, a Agência aplica uma coima de 200.000 euros.

Uma instituição financeira sancionada em 2.000.000 de euros por exigir o consentimento de um cliente para o tratamento dos seus dados como requisito para contratar uma conta bancária

A AEPD, na sua decisão PS/00531/2023, aplicou uma coima de 2.000.000 de euros a uma instituição financeira que, para que os seus clientes pudessem finalizar a contratação de um determinado tipo de conta bancária, exigiu que estes prestassem o seu consentimento para que a entidade solicitasse à Tesouraria Geral da Segurança Social informação sobre a sua atividade económica, para dar cumprimento ao disposto na Lei 10/2010, de 28 de abril, relativa à prevenção do branqueamento de capitais e do financiamento do terrorismo.

Esta lei estabelece a obrigação de verificar as atividades profissionais e comerciais das entidades com as quais se pretende fazer negócios, mas não prevês que tal deva ser feito de uma forma específica. Embora o consentimento possa ser uma opção, a AEPD entende que a sua implementação não foi adequada, uma vez que o consentimento não pode ser considerado uma base jurídica válida se a celebração de um contrato estiver sujeita à sua concessão.

A autoridade de controlo da proteção de dados irlandesa aplica uma coima de 530.000.000 de euros ao TikTok pela realização de transferências internacionais irregulares

Em 2 de maio, a autoridade de supervisão irlandesa emitiu um comunicado de imprensa anunciando a imposição de uma coima de 485.000.000 de euros ao TikTok por realizar transferências internacionais para a China sem uma avaliação adequada do impacto dessas transferências, o que impossibilitava a adoção de garantias adequadas.

Além disso, embora o TikTok tenha corrigido em 2022 as violações detetadas na sua política de privacidade para os titulares de dados no Espaço Económico Europeu, no âmbito da investigação, a autoridade de controlo impôs uma coima de 45.000.000 de euros por violação do seu dever de informar durante o período compreendido entre 29 de julho de 2020 e 1 de dezembro de 2022.

As duas sanções totalizam 530.000.000 de euros, mais a obrigação de regularizar as transferências nos próximos seis meses ou, caso contrário, suspender a sua realização.

A AEPD sanciona o Ministério para a Transição Ecológica e o Desafio Demográfico (MTERD)

A Fundação Éticas Data Society denunciou à AEPD que o "sistema de informação BOSCO" utilizado pelo MTERD para determinar a concessão do apoio social da eletricidade toma decisões automatizadas, sem intervenção humana significativa, sem controlos de qualidade periódicos ou mecanismos adequados para que as partes interessadas possam contestar ou exprimir o seu ponto de vista. Além disso, foram destacadas a falta de transparência quanto às informações fornecidas aos titulares dos dados sobre o tratamento e a ausência de uma avaliação de impacto sobre a proteção de dados (AIPD).

Embora o Ministério defenda a existência de participação humana na gestão dos pedidos e no tratamento das reclamações, bem como a implementação de códigos de observação para reportar os motivos do indeferimento, a AEPD, na sua decisão de 9 de maio de 2025 PS-00324-2025, declara: (i) violado o artigo 22.º do RGPD, uma vez que o sistema BOSCO adota decisões automatizadas sobre a atribuição do apoio social sem cumprir os requisitos exigidos; (ii) a violação do artigo 35.º do RGPD, por não realizar uma AIPD; e (iii) a violação do artigo 13.º do RGPD, ao não informar os titulares dos dados sobre a existência de decisões automatizadas ou sobre os seus direitos associados. Consequentemente, a AEPD aplica uma série de medidas corretivas, incluindo a obrigação de informar os titulares dos dados sobre as decisões automatizadas e de realizar uma AIPD no prazo máximo de seis meses, bem como a garantia do direito à intervenção humana no prazo máximo de nove meses.

A AEPD sanciona o Conselho Geral do Notariado (CGN) por exigir e arquivar cópia do documento de identificação (DNI) dos requerentes no Portal Notarial do Cidadão

O reclamante apresentou uma reclamação à AEPD, alegando que o Portal Notarial do Cidadão exigia uma fotografia de frente e verso do DNI (Documento Nacional de Identidade) para o registo, o que considerava excessivo e desnecessário, uma vez que a assinatura eletrónica era suficiente.

Na sua decisão de 6 de maio de 2025 PS-00052-2024, a AEPD declara a ilicitude do tratamento e a violação do n.º 1 do artigo 6.º do RGPD, uma vez que: (i) embora o notário esteja obrigado a verificar a documentação que comprove a identificação do titular dos dados (como o DNI), a sua conservação só é obrigatória nos casos previstos na Lei 10/2010 relativa à prevenção do branqueamento de capitais e do financiamento do terrorismo; e (ii) o consentimento recolhido não cumpriu os requisitos do RGPD para ser considerado válido. Além disso, a AEPD sublinha que o CGN não cumpriu o dever de fornecer informações previsto no artigo 13.º do RGPD, porque a política de privacidade não diferenciou adequadamente as bases legais ou as finalidades do tratamento (particularmente no que diz respeito à retenção da cópia do DNI). Por último, a AEPD declara que o Encarregado da Proteção de Dados (DPO) do CGN, que é a Agência Notarial de Certificação (ANCERT), violou o dever de independência exigido pelo artigo 38.º, n.º 6 do RGPD, uma vez que atuou simultaneamente como subcontratante e DPO, o que constitui um conflito de interesses. Consequentemente, a AEPD determina a adoção de medidas corretivas para adequar o tratamento de dados à

regulamentação aplicável e a sua comprovação no prazo de seis meses.

Uma farmácia sancionada em 16.000 euros por três infrações do RGPD

A farmácia recolhia e armazenava os dados pessoais e de saúde dos doentes (nome, apelido, CIPA, CIP, medicação, médico prescritor, centro de saúde, etc.) em ficheiros Excel para renovar medicamentos sem a presença do doente ou do seu cartão de saúde. Este tratamento foi realizado sem garantias de proteção suficientes, uma vez que os ficheiros eram armazenados nos computadores da farmácia, protegidos apenas por uma palavra-passe partilhada por todos os funcionários, e os computadores estavam em balcões visíveis para os clientes. Além disso, o tratamento foi realizado sem o consentimento informado do paciente, uma vez que não foi fornecida qualquer informação específica sobre o tratamento dos seus dados pessoais.

Na sua decisão de 5 de maio de 2025 PS-00187-2025 a AEPD aplicou uma coima total de 16.000 euros por violação dos artigos 13.º, n.º 9 e 32.º do RGPD. Relativamente ao dever de informação (artigo 13.º do RGPD), a AEPD considerou que a farmácia não prestou informação aos titulares dos dados sobre o tratamento dos seus dados pessoais, violando o princípio da transparência, tendo, por isso, aplicado uma coima de 3000 euros. Em relação ao tratamento de dados de saúde (artigo 9.º do RGPD), a AEPD entendeu que os dados de saúde foram tratados sem uma base jurídica adequada, sem consentimento explícito e sem que tenha ocorrido nenhuma das exceções do artigo 9.º, n.º 2 do RGPD e, por conseguinte, aplicou uma coima de 10.000 euros. No que respeita à segurança do tratamento (artigo 32.º do RGPD), a AEPD considerou que não foram adotadas medidas técnicas e organizativas adequadas para garantir a segurança dos dados, com potencial acesso não autorizado e ausência de controlo sobre os ficheiros, tendo, por isso, aplicado uma coima de 3000 euros.

Após a notificação da decisão inicial, a farmácia reconheceu a responsabilidade e pagou voluntariamente a coima.

Sancionado por cumprir indevidamente a obrigação do registo de hóspedes

O reclamante reservou um apartamento turístico através de uma plataforma e foi forçado a utilizar uma aplicação de check-in online que exigia que fotografasse ambos os lados do seu documento de identidade e enviasse uma fotografia do rosto (*selfie*) para aceder ao alojamento. Na sua decisão de 8 de maio de 2025 PS-00546-2024, a AEPD aplica uma sanção total de 2500 euros, que corresponde a 1000 euros por infração da alínea c) do n.º 1 do artigo 5.º do RGPD e 1500 euros por infração do artigo 9.º do RGPD.

Em relação ao princípio da minimização de dados (artigo 5.º, n.º 1, alínea c) do RGPD), a AEPD conclui que a regulamentação do setor exige a recolha e comunicação de determinados dados (nome, apelido, número do documento de identidade, nacionalidade, data de nascimento, etc.), mas não a imagem completa do documento de identidade ou a fotografia facial do hóspede, pelo que o tratamento de dados pessoais não é legítimo. Em relação ao tratamento de dados biométricos (artigo 9.º do RGPD), a AEPD considera que, uma vez que a verificação biométrica facial constitui um tratamento de dados de categoria especial (proibido, a menos que se aplique uma das exceções do artigo 9.º, n.º 2 do RGPD) e nenhuma das exceções do artigo 9.º, n.º 2 do RGPD se verifica, o tratamento de dados biométricos foi realizado sem uma base legal. Além disso, a AEPD esclarece que a obrigação legal de registar os hóspedes não abrange a recolha excessiva de dados nem o tratamento de dados biométricos, e que a verificação da identidade pode ser realizada através de outros meios menos invasivos.

A Autoridade Polaca de Proteção de Dados aplica sanção de 132.000 euros porque o DPO de uma empresa não exercia a sua independência de forma plena e não incluiu a elaboração de perfis no RAT nem na PIA

Na sua decisão de 18 de novembro de 2024, a Autoridade de Controlo polaca aplicou uma coima de 132.000 euros a uma instituição bancária pela infração dos artículos 30.º, 35.º e 38.º do RGPD. Após uma investigação, a Autoridade de Controlo descobriu que, embora o banco tenha criado perfis de vários dados de clientes para determinar a sua solvência e posteriormente tratado a pontuação creditícia daí resultante, esses tratamentos não foram incluídos no seu registo de atividades de tratamento de dados. Além disso, o banco não realizou uma avaliação de impacto sobre a proteção de dados e, por conseguinte, não avaliou as implicações da criação de perfis para a segurança do tratamento de dados pessoais. No entanto, o banco corrigiu esta violação antes do início da investigação.

Além disso, foi revelado um conflito de interesses na função do Encarregado da Proteção de Dados (DPO) nomeado pelo banco. O DPO não exerceu plenamente a independência exigida pelo RGPD porque não reportava diretamente à direção de topo do banco, ou seja, ao Conselho de Administração, e, além disso, trabalhava como auditor informático/especialista de segurança no Departamento de Segurança, reportando diretamente ao Diretor desse departamento.

A AEPD aplica uma coima de 10.000 euros a uma marca de cosméticos por violação do artigo 22.º, n.º 2 da LSSI

O processo PS-531/2024 é iniciado com uma denúncia de um reclamante sobre a instalação de cookies não técnicos sem consentimento no site da parte sancionada.

A entidade denunciada alega que o problema ocorreu devido a uma omissão nos controlos de implementação de cookies de terceiros e que foram adotadas medidas corretivas para o resolver (bloqueio de vídeos integrados, atualização da política de cookies, integração de um CMP, reforço de auditorias, etc.). No entanto, a AEPD detetou vários problemas no comportamento dos *cookies* do site: (i) o painel de gestão de *cookies* tinha as opções pré-definidas como "ON", o que não é aceitável; (ii) mesmo após rejeitar *cookies* não essenciais, o site continuou a instalar cookies de segmentação e de desempenho; (iii) não existia um mecanismo acessível e permanente para modificar o consentimento durante a navegação; e (iv) a informação sobre a gestão de *cookies* foi limitada às instruções para o navegador, o que não é suficiente como único mecanismo.

Em conclusão, a AEPD considera que existiu uma violação do artigo 22.º, n.º 2 da LSSI com base na instalação de *cookies* não técnicos ou necessários sem consentimento prévio, na instalação de *cookies* não técnicos mesmo após rejeição expressa e na ausência de um mecanismo para modificar ou retirar o consentimento a qualquer momento. Assim, é aplicada uma coima de 10.000 euros por infração ligeira ao artigo 22.º, n.º 2 da LSSI, agravada pela reincidência, uma vez que a entidade já foi sancionada por atos semelhantes em 2023.

O TJUE confirma a determinação das sanções do RGPD segundo o conceito de 'empresa' do direito da concorrência

No dia 13 de fevereiro, o Tribunal de Justiça da União Europeia (TJUE) publicou o acórdão do processo C-383/23, que resolveu uma questão prévia suscitada pelo Tribunal de Recurso da Região Oeste da Dinamarca no recurso interposto por uma cadeia dinamarquesa de lojas de mobiliário contra o montante da coima administrativa que lhe foi aplicada por violação do prazo de conservação de dados pessoais.

Inicialmente, a cadeia foi sancionada em 200.000 € por violação do artigo 5.º, n.º 1, alínea e) do RGPD, valor calculado com base no volume de negócios do grupo empresarial a que pertencia. Ao analisar este volume para calcular a coima, as autoridades dinamarquesas consideraram necessário aplicar o conceito de empresa utilizado no direito da concorrência, que considera uma empresa como uma "unidade económica".

O TJUE responde com base no artigo 83.º do RGPD, que estabelece que as coimas devem ser proporcionais e dissuasoras. Distingue ainda entre o cálculo do valor máximo da coima e a sua proporcionalidade. Sem prejuízo do exposto, o Tribunal indica que a definição de “empresa” deve estar em consonância com os artigos 101.º e 102.º do Tratado sobre o Funcionamento da União Europeia (TFUE), ou seja, com a definição de unidade económica no âmbito do direito da concorrência.

O TJUE decide sobre o alcance do direito de acesso do titular dos dados e a lógica utilizada na adoção de decisões automatizadas

Uma empresa de telecomunicações austríaca rejeitou a prorrogação de um contrato com um cliente com base numa avaliação automatizada da sua solvência, que concluiu que o cliente não tinha classificação creditícia suficiente para assinar o contrato. O cliente contactou a autoridade austríaca de proteção de dados, que ordenou à empresa que fornecesse informações significativas sobre a lógica aplicada na decisão automatizada.

A empresa recorreu da ordem, argumentando que não estava obrigada a divulgar mais informações devido a segredos comerciais, e o tribunal austríaco competente concluiu que a empresa tinha violado o RGPD ao não fornecer informações suficientes sobre a lógica do processo automatizado. No entanto, o pedido de execução desta decisão foi rejeitado pela autoridade de execução de Viena, que considerou que a empresa tinha cumprido suficientemente a sua obrigação de informação.

A titular dos dados recorreu para o tribunal remetente, que submeteu questões prejudiciais ao TJUE. Estas questões centraram-se na interpretação do artigo 15.º, n. 1, alínea h) do RGPD, que estabelece que o titular dos dados tem o direito de obter informações significativas sobre a lógica envolvida na tomada de decisão automatizada, incluindo a criação de perfis.

Na sua decisão do processo C-203/22, o Tribunal de Justiça esclareceu que, no caso de decisões automatizadas, o responsável pelo tratamento deve explicar de forma concisa, transparente, inteligível e facilmente acessível o procedimento e os princípios aplicados ao tratamento dos dados pessoais do titular dos dados. Além disso, se as informações incluírem dados protegidos de terceiros ou segredos comerciais, o responsável pelo tratamento deverá comunicar essas informações à autoridade de supervisão ou ao tribunal competente, que ponderará os direitos e interesses em causa para determinar o âmbito do direito de acesso do titular dos dados.

O TJUE reconhece o direito de retificação sobre os dados relativos ao sexo da pessoa sem necessidade de demostrar a realização de uma cirurgia de mudança de sexo

Após uma decisão preliminar apresentada por um tribunal húngaro, ocorre o caso de uma pessoa que solicitou que o seu nome e sexo fossem corrigidos no registo nacional de asilo húngaro, fornecendo atestados médicos comprovativos da sua identidade de género como sendo do sexo masculino. No entanto, a administração rejeitou o pedido porque a cirurgia de mudança de sexo não tinha sido comprovada.

Na sua decisão sobre este caso (C-247/23), o TJUE decidiu que, nos termos do artigo 16.º do RGPD, uma pessoa tem o direito de retificar dados pessoais relativos ao seu sexo sem ter de provar que foi submetida a uma cirurgia de mudança de sexo, sendo suficientes os atestados médicos que comprovem a sua identidade, em conformidade com o princípio da exatidão dos dados. Acrescenta que um Estado-Membro não pode condicionar o exercício do direito à rectificação à existência de um procedimento nacional de reconhecimento de género nem exigir uma cirurgia, pois tal violaria os direitos à integridade e à privacidade reconhecidos na Carta dos Direitos Fundamentais da UE.

O Advogado-Geral do TJUE emite parecer sobre o processo C-654/23 relativo à relação entre o RGPD e a Diretiva ePrivacy

No parecer emitido no âmbito do processo C-654/23, Inteligo Media SA vs Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Carácter Personal (ANSPDCP), em resposta ao pedido de decisão prejudicial apresentado pelo Tribunal Superior de Bucareste, o Advogado-Geral Szpunar, no seu parecer, sustenta que a prestação de um serviço aparentemente gratuito para fins publicitários pode constituir uma forma de comercialização direta na aceção do artigo 13.º da Diretiva relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva 2002/58/CE). Consequentemente, o envio de *newsletters* sem consentimento prévio seria lícito se os requisitos do n.º 2 do artigo 13.º da referida Diretiva fossem cumpridos, sem necessidade de recorrer ao artigo 6.º do Regulamento Geral de Proteção de Dados (RGPD) como base jurídica adicional.

O caso analisado diz respeito a um site que oferecia acesso gratuito limitado a conteúdos, expansível através do registo de e-mail, enquanto o acesso total exigia pagamento. Após o registo, o utilizador — sem subscrever o plano pago — recebia uma *newsletter* com novidades do site.

O Advogado-Geral conclui que essa *newsletter* constitui comercialização direta, uma vez que o modelo económico (*soft paywall*) procura induzir o utilizador a adquirir um serviço pago. Considera-se que o fornecimento de dados pessoais (como o endereço de correio eletrónico) em troca de

conteúdo pode ser entendido como uma contrapartida por um serviço, enquadrando-se no conceito de "venda" do n.º 2 do artigo 13.º. Esta disposição seria exaustiva, pelo que não seria necessária qualquer base adicional ao abrigo do RGPD. Além disso, realça que o RGPD e a Diretiva ePrivacy respondem a diferentes direitos fundamentais e são compatíveis e complementares na sua aplicação.

O TSJ da Extremadura confirma o despedimento legítimo de uma vigilante por divulgar dados pessoais num grupo de WhatsApp

O Tribunal Superior de Justiça da Extremadura confirmou o despedimento com justa causa de uma vigilante do Centro Penitenciário de Badajoz por, entre outros motivos, uma grave violação das normas de proteção de dados. A trabalhadora foi despedida depois de se ausentar do seu posto durante nove minutos enquanto o sistema de alarme estava desativado, violando o protocolo de passagem de turnos. A empresa deu-lhe 48 horas para apresentar os seus argumentos, e a funcionária respondeu por escrito, justificando as suas ações por questões de saúde e acusando o seu superior hierárquico de assédio no local de trabalho.

No entanto, esta declaração escrita de alegações — que incluía informações pessoais sobre colegas, referências a turno, protocolos internos e informações operacionais do centro — foi posteriormente partilhada pela própria trabalhadora num grupo de WhatsApp chamado "Grupo Extremadura VS", com quase 400 participantes externos à empresa. O tribunal concluiu que esta divulgação não autorizada constituía uma violação muito grave do seu dever de confidencialidade e uma violação dos regulamentos de proteção de dados pessoais.

A Secção Social, no seu acórdão 31/2025 de 21 de janeiro de 2025, Rec. 795/2024, indefere o recurso da trabalhadora por falta de base factual e jurídica suficiente, confirmando assim a sentença da instância inferior e declarando legítimo o despedimento, sem direito a indemnização ou processamento de salários.

A Audiência Nacional confirma coima de 40.000 euros a uma financeira por tratar dados de uma vítima de roubo de identidade sem fundamento legal

A Audiência Nacional confirmou a sanção de 40.000 euros aplicada pela Agência Espanhola de Proteção de Dados (AEPD) a uma empresa que se dedica à gestão e recuperação de créditos por uma infração muito grave da legislação de proteção de dados. A empresa tratou os dados pessoais de um titular de dados que foi vítima de roubo de identidade na contratação fraudulenta de um empréstimo sem uma base legítima para tal tratamento, em violação do Artigo 6.º, n.º 1, alínea b) do Regulamento Geral de Proteção de Dados (RGPD).

Embora a parte afetada tenha comunicado o roubo de identidade e solicitado a eliminação dos seus dados em março de 2021, a entidade não os removeu do registo de dívidas da ASNEF até quase dois meses depois, continuando a tratar os seus dados sem consentimento nem motivo justificativo. A Secção de Contencioso Administrativo, 1.º Juízo, no acórdão de 13 de fevereiro de 2025, Rec. 1005/2022, rejeita que tenha sido exercida a diligência devida e afasta a aplicação da isenção prevista no artigo 4.º, n.º 2, alínea a) da LOPD-gdd, uma vez que os dados não eram exatos nem provinham diretamente do interessado.

O tribunal realçou que o consentimento deve ser inequívoco e que a empresa é responsável pelo tratamento mesmo após a cessão do crédito. O recurso da instituição financeira é negado e esta é condenada no pagamento das custas do processo.

A Audiência Nacional reconhece o direito de acesso a dados pessoais bloqueados em registos de incumprimento

A Secção de Contencioso Administrativo, 1.º Juízo, da Audiência Nacional, no seu acórdão de 13 de fevereiro de 2025, Rec. 2255/2021, negou provimento ao recurso interposto por uma entidade gestora de um registo de dívidas contra a decisão da AEPD que reconheceu o direito de um cidadão ao acesso aos dados pessoais bloqueados nos seus sistemas.. Embora os dados estivessem cancelados e bloqueados desde março de 2019, em janeiro de 2021 a parte afetada solicitou o acesso à informação sobre a sua inclusão anterior no ficheiro, assim como informações sobre as entidades que consultaram os seus dados e o motivo do seu cancelamento.

A entidade negou parte da informação solicitada, argumentando que os dados bloqueados não podem ser visualizados ou tratados, exceto pelas autoridades públicas nos casos previstos na lei. No entanto, a Audiência Nacional apoia a posição da AEPD ao declarar que facultar ao titular dos dados o acesso aos seus próprios dados bloqueados — dados tratados durante a relação contratual — não constitui uma operação de tratamento ao abrigo do RGPD e da LOPD-gdd.

O tribunal sublinha que o direito de acesso persiste mesmo após o bloqueio dos dados, desde que não tenham sido fisicamente eliminados. Esta interpretação garante o controlo da parte afetada sobre a sua informação e não viola o princípio de limitação do período de conservação. As custas processuais são imputadas à entidade recorrente.

Uma instituição bancária e uma gestora de registos são condenadas por interferência ilegal na honra de um consumidor

No acórdão 259/2024 de 20 de dezembro de 2024, Rec. 367/2022, a Audiência Provincial de Toledo confirma a condenação de uma instituição bancária e de uma entidade gestora de um registo de incumprimento por interferência ilegal no direito à honra de um consumidor, pela sua inclusão indevida no referido registo de devedores. O tribunal considera provado que não foram cumpridos os requisitos legais estabelecidos pela regulamentação de proteção de dados em vigor à data dos factos, como o pedido prévio de pagamento e a adequada notificação contratual sobre a inclusão nos sistemas de informação creditícia.

A entidade gestora do registo, enquanto entidade responsável pelo mesmo, alegou que a sua atuação era meramente técnica e que agiu de acordo com as instruções do credor. No entanto, o tribunal, seguindo a doutrina do Supremo Tribunal, sustenta que o titular do registo deve verificar a exatidão, relevância e legalidade dos dados antes de os conservar, não podendo simplesmente atuar de forma passiva. Esta falta de diligência devida constituiu um incumprimento das normas e uma violação do direito fundamental à proteção de dados.

Ambas as entidades foram condenadas solidariamente a pagar 10.000 euros por danos morais, tendo a entidade que gere o registo sido também condenada a apagar os dados do titular dos dados. A decisão enfatiza a responsabilidade ativa do responsável pelo tratamento de dados e a necessidade de proteger rigorosamente os dados pessoais contra interferências indevidas.

Um tribunal de Múrcia ordena a limpeza dos registos de dívidas depois de conceder a exoneração do passivo a um devedor

No despacho de 3 de maio de 2024, Recurso 79/2024, o Tribunal Comercial n.º 2 de Múrcia concedeu aos devedores a exoneração do passivo restante e, como efeito direto disso, ativou o mecanismo de proteção de dados previsto no artigo 492.º-ter do Texto Consolidado da Lei da Insolvência (TRLC). Esta regra estabelece que a decisão judicial que concede a exoneração deve

incluir uma ordem aos credores afetados para que comuniquem a exoneração aos sistemas de informação de crédito (registos de incumprimento) a que tenha sido comunicado anteriormente o não pagamento ou o atraso no pagamento das dívidas exoneradas.

A finalidade desta obrigação é atualizar os registos, garantindo que a informação negativa não é mantida indevidamente em prejuízo do devedor. Isto protege o seu direito à exatidão e atualização dos seus dados pessoais, de acordo com o artigo 5.º, n.º 1, alínea d) do RGPD. Da mesma forma, o devedor tem a possibilidade de obter uma cópia da decisão para solicitar diretamente a atualização dos seus dados nestes sistemas, reforçando o seu direito de acesso, retificação e apagamento.

Esta decisão sublinha a importância do princípio da minimização do tratamento e a necessidade de garantir que os dados relativos a créditos já exonerados não sejam utilizados ilegitimamente nem continuem a afetar a solvência do devedor, promovendo assim a depuração eficaz dos registos de incumpridores.

O TJUE esclarece que a publicitação de procedimentos de pagamento constitui uma oferta promocional protegida pela Diretiva de Comércio Eletrónico

O artigo 6.º, alínea c), da Diretiva 2000/31/CE relativa ao comércio eletrónico estabelece que as ofertas promocionais, tais como descontos, prémios e presentes, quando permitidas no Estado-Membro onde o prestador de serviços está estabelecido, devem ser claramente identificáveis como tal, e as condições a cumprir para aceder às mesmas devem ser facilmente acessíveis e apresentadas de forma clara e inequívoca.

O litígio (processo C-100/24) opõe uma associação de consumidores a um retalhista de moda especializado na venda por catálogo, que publicou no seu site uma mensagem publicitária relativa a um método de pagamento específico. Em concreto, o anúncio incluía uma mensagem que dizia "compra conveniente por conta". A associação de defesa do consumidor considerou que existia uma prática comercial desleal, mais concretamente uma omissão enganosa, ao não incluir na mensagem publicitária que, para ter acesso a esta opção, era necessário submeter-se a uma avaliação de crédito.

Quando o caso foi levado ao Tribunal Superior Regional Cível e Penal de Hamburgo, foi tomada uma decisão prejudicial sobre se a publicidade de um método de pagamento (neste caso, "compra conveniente por conta"), que tem um baixo valor monetário, mas serve a segurança e o interesse jurídico do consumidor, constitui uma oferta promocional para efeitos do artigo 6.º, alínea c), da Directiva 2000/31/CE relativa ao comércio eletrónico.

O tribunal determinou que uma oferta comercial deve ser entendida como qualquer comunicação através da qual um prestador de serviços procura promover bens ou serviços, proporcionando ao destinatário uma vantagem objetiva e certa que possa influenciar o seu comportamento na escolha de tais bens ou serviços. A forma que essa vantagem assume, bem como o seu significado, são irrelevantes; podendo ser, em particular, uma vantagem pecuniária ou jurídica ou uma mera conveniência, como, por exemplo, permitir ao destinatário poupar tempo.

O TJUE enfatizou ainda a importância de uma interpretação teleológica da norma, indicando que o objetivo da directiva é garantir um elevado nível de protecção do consumidor.

Por último, o Tribunal concluiu que uma mensagem publicitária que mencione um método de pagamento específico pode, de facto, ser considerada uma oferta publicitária na medida em que

proporcione ao destinatário dessa mensagem uma vantagem objetiva e certa que possa influenciar o seu comportamento na escolha de um bem ou serviço.

O Tribunal do Mercado da Bélgica confirma a sanção imposta à IAB Europe e a sua responsabilidade conjunta pela gestão do "Transparency & Consent Framework"

Após a decisão do TJUE sobre as questões prejudiciais suscitadas pelo Tribunal do Mercado da Bélgica relativamente à validade do *Transparency & Consent Framework* (TCF) da IAB Europe, o tribunal proferiu um acórdão. Mais importante ainda, este declara a corresponsabilidade da IAB Europe pela criação de cadeias de consentimento que armazenam as preferências dos utilizadores em relação à utilização dos seus dados no ecossistema publicitário.

Em fevereiro de 2022, a autoridade belga de proteção de dados declarou que a associação acima referida, que desenvolveu o TCF como uma estrutura de autorregulação para o mercado da publicidade online, era corresponsável pela criação das cadeias de consentimento e pelas suas posteriores utilizações, impondo uma coima de 250.000 euros..

A IAB Europe recorreu da decisão para o Tribunal do Mercado da Bélgica, que remeteu uma série de questões prejudiciais para o TJUE, que foram decididas em março de 2024, declarando que as cadeias de consentimento contêm dados pessoais e que a IAB Europe é corresponsável pela sua criação, mas não por qualquer utilização subsequente que outras partes possam fazer desses dados.

Com estas questões esclarecidas, o Tribunal do Mercado da Bélgica decidiu agora no mesmo sentido, limitando a corresponsabilidade da IAB Europe a certos aspetos da operação do TCF, mantendo a coima de 250.000 euros inicialmente imposta e mantendo a necessidade de implementar um plano de ação para garantir o cumprimento do RGPD.

A Audiência Nacional decide sobre a sanção multimilionária imposta pela AEPD a uma instituição bancária em 2021

Esta decisão aplicava sanções por violações de obrigações de transparência (2.000.000 de euros), e pela falta de base jurídica suficiente para determinados tratamentos de dados pessoais por parte da instituição financeira (4.000.000 de euros).

Após recurso da decisão da AEPD pela parte sancionada, a Audiência Nacional, na sua decisão sobre o assunto, concorda com a AEPD na constatação de violações dos regulamentos aplicáveis, embora difira no tratamento jurídico da conduta observada, concedendo provimento parcial ao recurso da parte sancionada.

O aspeto mais notável desta decisão é que a Audiência Nacional considera que existe um concurso instrumental pelo qual as violações dos artigos 13.º e 14.º do RGPD, relacionadas com a transparência das informações prestadas aos titulares dos dados, são, até certo ponto, subsumidas na sanção imposta pela violação do artigo 6.º do RGPD sobre bases legais. Neste sentido, aprecia-se a prática de uma violação do artigo 6.º do RGPD em concurso instrumental com uma violação dos arts. 13.º e 14.º do RGPD, e aplica-se uma coima única de 2 milhões de euros.

Tal, na opinião da Audiência Nacional, deve-se ao facto de que, se as informações de proteção de dados fornecidas pela entidade sancionada nas suas políticas de privacidade estivessem completas e em total conformidade com os referidos artigos 13.º e 14.º do RGPD, o consentimento dos titulares dos dados (que funcionava como base legal aplicável neste caso) poderia ter sido validamente

obtido. Por outras palavras, a Audiência Nacional considera que o incumprimento do dever de transparência é um elemento essencial e inerente à violação do artigo 6.º do RGPD. Neste sentido, a sanção originária é significativamente reduzida.

Esta decisão pode ter implicações interpretativas importantes para o futuro. Este mesmo critério poderia ser aplicado a outras matérias, tais como potenciais concursos instrumentais entre a falta de implementação de medidas de segurança técnicas e organizacionais (artigo 32.º do RGPD) e o dever de integridade e confidencialidade (artigo 5.º do RGPD), violações que são frequentemente sancionadas de forma independente em casos de incidentes de segurança. Por conseguinte, será muito importante seguir de perto quaisquer alterações nos critérios da AEPD nas suas futuras resoluções.

4. Atualidade

As reformas em matéria de proteção de dados pessoais na América Latina e os seus efeitos nas relações laborais

Autores: Ricardo Eckardt, Jairo Jaller, Franco Muschi, Mariana Ubidia, Miguel Ángel Rocha e José Alberto González Rebolledo

Num novo ambiente onde a proteção de dados é priorizada acima de todas as outras necessidades empresariais, as empresas são forçadas a rever os processos e políticas internas, bem como a adotar medidas robustas para garantir a conformidade regulamentar e proteger as informações pessoais dos seus trabalhadores, candidatos e colaboradores. Dos processos de seleção às avaliações de desempenho e aos mecanismos de controlo laboral, o tratamento de dados pessoais tornou-se um foco central da gestão de pessoas. Além disso, a utilização de ferramentas de IA gera uma exposição significativa de informação pessoal — em muitos casos, sensível — o que exigirá, muitas vezes, a adoção de políticas que garantam a confidencialidade da informação que os departamentos de seleção e recrutamento passarão a utilizar.

As regulamentações na América Latina começaram a responder a esta realidade. O Peru, o México e o Chile já implementaram reformas regulamentares significativas relacionadas com a proteção de dados, enquanto na Colômbia a regulação data de 2012. No entanto, os empregadores e os trabalhadores tornaram-se gradualmente mais conscientes da importância e da sensibilidade do tratamento de dados pessoais. Este processo de assimilação e atualização normativa — que procura alinhar a legislação local com os padrões internacionais — exige um nível de exigência mais elevado para os empregadores e um controlo mais apertado por parte das autoridades.

A seguir apresentamos uma visão geral atualizada dos principais desenvolvimentos regulamentares e considerações práticas sobre a proteção de dados pessoais no local de trabalho no Peru, Colômbia, México e Chile.

Peru

A 30 de novembro de 2024, foi publicado o Decreto Supremo n.º 016-2024-JUS, que aprova o novo Regulamento da Lei de Proteção de Dados Pessoais (Lei n.º 29733), substituindo integralmente o regulamento anterior. Este regulamento entrou em vigor a 30 de março de 2025 e representa um marco na regulamentação peruana ao integrar normas internacionais e estabelecer novos requisitos para o tratamento de dados pessoais. No domínio laboral, introduz mudanças substanciais que exigem uma revisão e adaptação abrangente das práticas

empresariais relacionadas com a gestão de dados dos trabalhadores.

Como primeira questão relevante, a nova regulamentação reforça as principais obrigações dos empregadores no tratamento dos dados dos trabalhadores. Assim, a omissão de informação completa dos trabalhadores sobre o tratamento dos seus dados pessoais é considerada uma infração grave (penalizada com uma coima até aproximadamente USD 70.000,00), nos termos do artigo 18.º da Lei. Isto exige a revisão e adaptação de todos os documentos de informação laboral (políticas, formatos, cláusulas, etc.).

Da mesma forma, o tratamento fora de prazo dos direitos ARCO (acesso, retificação, cancelamento e oposição) é classificado como uma infração ligeira (até aproximadamente 7.000,00 USD), o que requer a revisão e o reforço dos procedimentos internos para o exercício dos direitos por parte dos trabalhadores.

Como novidade, é introduzido o requisito de nomeação de um encarregado dos dados pessoais quando se verifiquem determinadas condições. Os Recursos Humanos devem estar ativamente envolvidos nesta nomeação, pois pode envolver mudanças de funções, acesso a informação e condições de trabalho.

Por fim, o regulamento descreve novas medidas de segurança, como a exigência de um documento de segurança atualizado e distribuído internamente que inclua procedimentos de acesso, gestão de privilégios e utilização de plataformas, entre outros. A implementação adequada é essencial para minimizar os riscos legais, fortalecer uma cultura de cumprimento e promover a confiança dos trabalhadores na organização.

Colômbia

A proteção de dados pessoais tem vindo a tornar-se cada vez mais importante no ambiente empresarial, especialmente no âmbito laboral. Desde a aprovação da Lei Estatutária 1581 de 2012, que estabelece o regime geral de proteção de dados pessoais, e dos seus decretos regulamentares, as organizações são obrigadas a implementar medidas que garantam a privacidade, a segurança e o tratamento adequado das informações pessoais dos seus trabalhadores.

Nos últimos anos, a Superintendência da Indústria e Comércio (SIC), enquanto autoridade nacional nesta área, reforçou o seu papel de supervisão e sanção, emitindo novas instruções e decisões que exigem às empresas uma revisão permanente das suas políticas internas. Recentemente, a regulamentação de proteção de dados foi assimilada e interiorizada de forma mais consistente, e foram consolidadas diretrizes mais rigorosas sobre o tratamento de dados confidenciais, a responsabilidade comprovada e a gestão de bases de dados, o que levou a um regime de sanções mais rigoroso e a maiores exigências para a documentação de conformidade.

De entre as recentes emissões de normas e orientações, destacam-se as circulares externas emitidas pela Superintendência da Indústria e Comércio sobre o tratamento de dados pessoais. Entre elas contam-se a Circular Externa n.º 002, de 21 de agosto de 2024, que aborda o tratamento de dados pessoais em sistemas de inteligência artificial, e a Circular Externa n.º 003, de 22 de agosto do mesmo ano, que fornece instruções aos administradores das empresas sobre o tratamento desta informação.

No contexto laboral, estas disposições representam uma transformação significativa na forma como as empresas gerem a informação dos seus trabalhadores. Desde a obtenção do consentimento informado durante o processo de recrutamento até à implementação de medidas de cibersegurança, as organizações devem garantir que as suas práticas respeitam os direitos dos trabalhadores e estão alinhadas com os princípios da legalidade, finalidade, liberdade, veracidade, transparência, acesso e circulação restrita.

A autoridade tem procurado consistentemente emitir orientações e guias destinadas a orientar as empresas e os seus colaboradores no tratamento adequado dos dados pessoais. Estas ferramentas incluem folhetos e documentos técnicos sobre temas como a implementação do encarregado da conformidade da proteção de dados, bem como sobre atividades relevantes para as organizações, como a videovigilância e a sua gestão adequada de acordo com as normas em vigor.

Esta estrutura regulamentar não procura apenas proteger a privacidade dos trabalhadores, mas também promover uma cultura organizacional baseada na confiança, transparência e conformidade normativa. Assim, a proteção de dados pessoais tornou-se um pilar fundamental das relações laborais modernas na Colômbia.

México

A 20 de março de 2025, foi publicada no Diário Oficial da Federação uma nova Lei Federal sobre a Proteção de Dados Pessoais na Posse de Particulares. Esta legislação, que substitui a norma de 2010, introduz disposições mais claras e robustas para garantir o tratamento legítimo e seguro de informações pessoais no país. A seguir, exploramos os principais desenvolvimentos e o seu impacto no ambiente empresarial latino-americano.

Maior clareza e obrigações: a nova lei fortalece os direitos ARCO (Acesso, Retificação, Cancelamento e Oposição), agora definidos com precisão e explicitamente reconhecidos, ultrapassando a ambiguidade da legislação anterior. Além disso, impõe obrigações mais rigorosas às empresas e aos particulares que lidam com dados pessoais, sejam eles físicos, eletrónicos ou em qualquer outro formato. Entre os requisitos, destacam-se:

1. Avisos de privacidade mais detalhados: as empresas devem informar de forma clara e acessível sobre as finalidades do tratamento de dados, especificando: (i) que dados são recolhidos, incluindo dados sensíveis; (ii) quais exigem consentimento expresso e, (iii) como exercer os direitos ARCO.

2. Direito de oposição: os titulares dos dados podem opor-se ao seu tratamento se existir um motivo legítimo, como um dano ou prejuízo potencial, ou quando a utilização automatizada dos dados afetar os seus direitos, avaliar aspetos pessoais (desempenho no trabalho, situação económica ou saúde, entre outros) ou gerar efeitos jurídicos não desejados.

3. Confidencialidade obrigatória: as organizações devem implementar controlos para garantir que qualquer pessoa envolvida no tratamento de dados mantém a estrita confidencialidade.

4. Cultura de proteção de dados: as empresas devem promover a proteção de dados internamente, designando, se necessário, um responsável ou departamento para tratar dos pedidos relacionados com os direitos ARCO.

Nova abordagem institucional: uma das mudanças mais significativas é o desaparecimento do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) como organismo garante. Em vez deste, a Secretaria Anticorrupção e Bom Governo assumirá a supervisão, a verificação e as sanções relativas aos dados pessoais a nível federal. As deliberações desta Secretaria só poderão ser impugnadas através de recurso para tribunais especializados, sendo eliminada a possibilidade de recurso de anulação para o Tribunal Federal Administrativo.

Além disso, as sanções e os custos associados ao exercício dos direitos ARCO serão calculados com base na unidade de medida atual e a sua atualização, garantindo uma base económica atualizada.

Impacto no âmbito laboral: para as empresas do México e da região, esta reforma exige uma revisão urgente das suas práticas administrativas. Os empregadores deverão:

(i) atualizar os avisos de privacidade, contratos e regulamentos internos para cumprir a nova lei; (ii) implementar processos que garantam a transparência no tratamento dos dados dos trabalhadores e (iii) capacitar os seus colaboradores na proteção de dados para evitar riscos legais.

Estas mudanças não só reforçarão a confiança dos trabalhadores, como também posicionarão as empresas como participantes responsáveisnum ambiente onde a privacidade é uma prioridade global.

Chile

Após sete anos de debate legislativo, o Chile tem uma nova Lei de Proteção e Tratamento de Dados Pessoais (Lei 21.719), promulgada em dezembro de 2024 e que entrará em vigor no último mês de 2026. Esta lei representa um marco no alinhamento das regulamentações nacionais com as normas internacionais, especialmente o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, estabelecendo uma estrutura robusta e moderna para a gestão de dados pessoais no país.

A nova norma é de aplicação geral, abrangendo todas as pessoas singulares e coletivas. Entre as suas principais novidades está a criação da Agência de Proteção de Dados Pessoais, um organismo autónomo responsável pela emissão de instruções, interpretação da lei, fiscalização do seu cumprimento e aplicação de sanções. Esta estrutura institucional será fundamental para a implementação e supervisão adequadas do novo regime.

No âmbito laboral, a lei reconhece os trabalhadores como titulares de dados pessoais perante os seus empregadores. Isto significa que têm os seguintes direitos sobre a sua informação: acesso, retificação, eliminação, oposição, portabilidade e bloqueio de dados. Estes direitos são irrenunciáveis e devem ser respeitados em todas as relações laborais, reforçando a obrigação existente no artigo 154.º-ter do Código do Trabalho, que exige aos empregadores a manutenção da confidencialidade das informações privadas dos seus trabalhadores.

O tratamento de dados pessoais em contexto laboral poderá ser efetuado com o consentimento expresso do trabalhador, mas será também lícito quando necessário à execução do contrato de trabalho, ao cumprimento de obrigações legais ou à satisfação de interesses legítimos do empregador, desde que não sejam violados os direitos e liberdades do trabalhador. Deve ser dada especial atenção aos dados sensíveis, como os dados de saúde, que só podem ser tratados sob condições rigorosas e com maiores garantias.

Para as empresas, a entrada em vigor da lei implica a necessidade de rever e adaptar as suas políticas e procedimentos internos de tratamento de dados. Será essencial implementar medidas que garantam o cumprimento dos princípios orientadores da lei: legalidade, finalidade, proporcionalidade, qualidade, responsabilização, segurança, transparência e confidencialidade. Além disso, as empresas multinacionais devem prestar especial atenção aos novos requisitos para as transferências internacionais de dados, assegurando que os países de destino têm níveis de proteção adequados ou que existem garantias contratuais suficientes.

Neste período de transição até dezembro de 2026, as empresas devem antecipar a adaptação dos seus sistemas, formar as suas equipas e estar atentas às normas e diretrizes que a futura Agência de Proteção de Dados Pessoais irá emitir, o que conferirá maior clareza e sentido prático à lei.

É de extrema importância cumprir a lei, pois o incumprimento pode dar origem a penalizações significativas, com coimas que podem chegar às 20.000 UTM (aproximadamente 1.466.600 de euros), valor que pode triplicar em caso de reincidência. Isto sublinha a importância da gestão proativa e responsável dos dados pessoais, tanto para evitar riscos legais como para fortalecer a confiança dos trabalhadores e clientes na organização.

Em suma, a nova lei marca um ponto de viragem na proteção de dados no Chile, exigindo que as empresas assumam um compromisso real com a privacidade e a segurança da informação, especialmente no âmbito laboral. A preparação e adaptação atempadas serão essenciais para abordar com sucesso este novo cenário regulamentar.

Lorenzo Cotino Hueso e Francisco Pérez Bes tomam posse como presidente e vice-presidente, respetivamente, da AEPD

No dia 3 de março de 2025, Lorenzo Cotino Hueso e Francisco Pérez Bes tomaram posse como presidente e vice-presidente, respetivamente, da Agência Espanhola de Proteção de Dados (AEPD), numa cerimónia realizada na sede da Agência e presidida pelo Ministro da Presidência, Justiça e Relações com as Cortes, Félix Bolaños.

Durante o seu discurso, Lorenzo Cotino destacou os desafios impostos pelo "tsunami digital" para a privacidade, especialmente em áreas como os espaços digitais, a saúde e a inteligência artificial, e anunciou o desenvolvimento de um plano estratégico para os enfrentar. Por sua vez, Francisco Pérez Bes destacou o compromisso da AEPD com o envolvimento dos cidadãos, a transparência, a agilidade e a inovação, bem como com a colaboração institucional.

O Ministro Bolaños enfatizou o importante papel que os dois cargos desempenham num contexto de crescentes tensões entre tecnologia e privacidade, e anunciou que a Lei de Proteção de Menores em Ambientes Digitais será em breve aprovada em segunda passagem pelo Conselho de Ministros, iniciando assim o seu processo parlamentar.

A nomeação de ambos os responsáveis foi formalizada pelos Decretos Reais 142/2025 e 143/2025, respetivamente. O evento contou com a presença de autoridades como Manuel Olmedo, Rafael Simancas e o ex-diretor da AEPD, Mar España, bem como de representantes dos setores público e privado.

A AEPD participa numa ação europeia para analisar a aplicação do direito ao apagamento

A 5 de março de 2025, a Agência Espanhola de Proteção de Dados (AEPD) anunciou a sua participação numa ação europeia coordenada focada na análise do direito ao apagamento (artigo 17.º do RGPD), um dos direitos mais frequentemente exercidos pelos cidadãos e também um que gera mais reclamações junto das autoridades de proteção de dados. Mais concretamente, o processo será avaliado para determinar se é acessível, compreensível e eficaz para os cidadãos.

Esta iniciativa faz parte do plano de ação do Comité Europeu para a Proteção de Dados (CEPD) para 2025 e envolve 32 autoridades nacionais. A AEPD analisará como uma amostra de responsáveis pelo tratamento de dados, tanto no setor público como no privado, lidam com os pedidos de apagamento, identificando as melhores práticas e as possíveis deficiências.

Os resultados serão avaliados em conjunto e poderão levar a novas ações de controlo ou aplicação em cada país. Além disso, será produzido um relatório agregado que apresentará uma visão geral da conformidade no Espaço Económico Europeu, e os resultados serão utilizados para incentivar as melhores práticas e promover a aplicação consistente do direito ao apagamento em toda a Europa.

Esta ação reflete a prioridade do CEPD de garantir a proteção eficaz dos direitos fundamentais em ambientes digitais, especialmente em plataformas com elevado impacto na privacidade do utilizador. Esta é a quarta ação do Quadro Coordenado de Aplicação do CEPD, que procura reforçar a cooperação entre as autoridades. As ações anteriores abordaram o direito de acesso, a utilização de serviços na nuvem pelo setor público e o papel do encarregado da proteção de dados.

Luz verde para o anteprojeto de lei para regular a inteligência artificial em Espanha

O Governo aprovou o Anteprojeto de Lei de Regulação da IA, que procura garantir uma utilização ética, inclusiva e centrada nas pessoas. A norma adaptará o quadro jurídico espanhol ao Regulamento Europeu da IA, em vigor desde 2024 e já parcialmente aplicável, e será tramitado com urgência. Em breve, deverá ser aprovado definitivamente pelo Conselho de Ministros como um projeto de lei e depois submetido ao Parlamento para aprovação.

O texto estabelece, como elemento-chave, as autoridades que irão fiscalizar os sistemas proibidos e de risco elevado com base no seu âmbito de aplicação. Para os sistemas proibidos, a competência é atribuída à AEPD (biometria e fronteiras), à CGPJ (justiça), à Junta Eleitoral Central (processos democráticos) e à AESIA (restantes utilizações). Quanto aos sistemas de risco elevado, estão também envolvidos o Banco de Espanha (solvabilidade), a CNMV (mercados financeiros) e a Direção-Geral de Seguros (seguros).

Catalunha lança projeto piloto baseado em IA para auxiliar na elaboração de decisões judiciais

A Catalunha lançou um projeto pioneiro em Espanha utilizando inteligência artificial nos tribunais através do AI4JUSTICE, um assistente baseado em IA concebido para auxiliar os juízes na elaboração de decisões.

O sistema permite pesquisas semânticas de jurisprudência e fundamentos jurídicos, com o objetivo de agilizar a resolução de casos repetitivos, otimizando o tempo e permitindo que os juízes se concentrem em questões mais complexas.

Desde setembro de 2024, quatro juízes comerciais da Audiência de Barcelona utilizam o AI4JUSTICE em casos que envolvem cláusulas mínimas ("*suelo*") e reclamações por incidentes de voo. Os resultados iniciais mostram uma redução do tempo de elaboração de sentenças de duas horas para apenas vinte minutos, e a poupança anual projetada é de 12.000 horas e 552.000 euros por cada vinte juízes.

Governo aprova projeto de Lei de Proteção de Menores no Ambiente Digital

Esta lei foi elaborada pelos Ministérios da Juventude e da Infância, da Justiça, dos Direitos Sociais e da Transformação Digital. O projeto de lei apresentado em junho do ano passado integrou contributos de várias organizações públicas e privadas de Espanha, bem como da Comissão Europeia.

Entre outras medidas, o projeto introduz um aumento da idade mínima para redes sociais dos 14 para os 16 anos para plataformas como o Facebook, Instagram e TikTok (com as empresas obrigadas a implementar sistemas fiáveis de verificação de idade); um requisito para que os dispositivos móveis incluam sistemas de controlo parental por defeito, que serão ativados durante a configuração inicial; e a criminalização da criação e disseminação não autorizadas de imagens ou áudios manipulados por IA sexualmente explícitos ou gravemente humilhantes.

As penas para adultos que atraem menores online para fins sexuais também foram endurecidas, e os menores estão agora proibidos de aceder a mecanismos de recompensa aleatórios, conhecidos como "*loot boxes*", um sistema incluído em muitos videojogos.

O "Information Commissioner's Office" (ICO) publica o seu guia sobre anonimização e pseudonimização

O guia enfatiza a anonimização eficaz como um processo para tornar os dados pessoais não identificáveis, recomendando avaliações de risco periódicas e o teste de "*motivated intruder*" para garantir que os dados permanecem anónimos.

Para o ICO, o facto de os dados serem anonimizados ou pseudonimizados depende do contexto, adotando-se, neste sentido, a doutrina subjetiva do TJUE, que estabelece que a capacidade do responsável pelo tratamento dos dados para concluir se são anonimizados ou pseudonimizados deve ser avaliada com base em saber se, em cada caso concreto, o responsável dispõe de meios razoáveis para identificar a pessoa. O que pode ser anónimo para uma pessoa pode não o ser para outra que, no contexto específico, tem a capacidade de reidentificar a partir de dados pseudonimizado.

A orientação recomenda ainda que as organizações adotem uma abordagem abrangente da governação ao anonimizar ou partilhar dados anonimizados, incluindo através de medidas como a realização de avaliações de impacto sobre a proteção de dados (AIPD) para documentar decisões de anonimização e identificar riscos e mitigações, coordenando-se com outras organizações que possam tratar dados relacionados que afetam a identificabilidade e definindo mecanismos e responsabilidades de controlo.

A Comissão Europeia publica um projeto de regulamento sobre as Normas Técnicas de Regulamentação para a subcontratação nos termos do Regulamento DORA

A Comissão Europeia publicou no passado dia 24 de março um projeto de regulamento em que se estabelecem as Normas Técnicas de Regulamentação para a subcontratação nos termos do Regulamento DORA, que inclui normas para a subcontratação de serviços de TIC que apoiam funções críticas ou importantes.

Estas obrigações incluem regras sobre proporcionalidade, aplicação para grupos, *due diligence*, avaliação de risco, descrição e condições da subcontratação e alterações materiais nos acordos e direitos de resolução das instituições financeiras. Além disso, especifica que as instituições financeiras devem ser informadas sobre alterações materiais nos acordos de subcontratação e que têm o direito de se opor ou resolver contratos se as tolerâncias de risco forem ultrapassadas ou ocorrer subcontratação não autorizada.

A empresa 23andMe declarada insolvente após uma violação de segurança em 2023

A empresa americana 23andMe, especializada em análise de ADN e testes genéticos diretos ao consumidor, declarou-se insolvente após anos de perdas financeiras e após o grave incidente de cibersegurança que comprometeu os dados pessoais de milhões de utilizadores em 2023. A 23andMe recolheu informação genética de mais de quinze milhões de pessoas.

Após a declaração de insolvência, a 23andMe anunciou que irá procurar uma venda, o que significa que a empresa, e com ela a informação genética dos seus 15 milhões de clientes, estarão provavelmente disponíveis no mercado em breve. A empresa afirma que não irá alterar a forma como gere ou protege os dados dos seus clientes e afirma que a privacidade dos dados será um fator importante em qualquer potencial transação.

No entanto, o Procurador-Geral de Nova Iorque emitiu recomendações sobre este assunto, instruindo os consumidores a eliminar os dados genéticos fornecidos à empresa e a destruir quaisquer amostras de ADN fornecidas.

O CEPD publica um relatório sobre os riscos dos grandes modelos de linguagem e a sua mitigação

Em 10 de abril, o CEPD publicou um relatório com orientações e ferramentas para gerir os riscos de privacidade em sistemas baseados em modelos de linguagem. A metodologia ajuda a identificar, avaliar e mitigar os riscos de privacidade e proteção de dados, apoiando o desenvolvimento responsável.

As orientações suportam os artigos 25.º e 32.º do RGPD, oferecendo medidas de segurança

e proteção de dados. No entanto, a adoção de tais medidas não substitui, por si só, a Avaliação de Impacto sobre a Proteção de Dados (AIPD), nos termos do artigo 35.º do RGPD, mas antes, quando aplicável, complementa-a.

Publicadas orientações europeias sobre o tratamento de dados pessoais com recurso a tecnologias de "blockchain"

O Comité Europeu para a Proteção de Dados publicou as Orientações 02/2025, que neste momento se encontram em fase de consulta pública. O CEPD destaca a complexidade e a incerteza do *blockchain* em relação ao tratamento de dados pessoais, o que representa desafios específicos para cumprir o RGPD. É crucial avaliar os riscos para os direitos e liberdades dos titulares dos dados, mitigando alguns deles através de medidas técnicas.

As propriedades do *blockchain* podem dificultar o cumprimento de requisitos como o direito de retificação e o direito a ser esquecido. As orientações fornecem um quadro para que as organizações avaliem cuidadosamente a utilização do *blockchain* e as responsabilidades dos agentes envolvidos.

A AEPD publica um parecer sobre a prorrogação da decisão de adequação do Reino Unido

Em junho de 2021, a Comissão Europeia adotou duas decisões de adequação para o Reino Unido, uma ao abrigo do RGPD e outra ao abrigo da Diretiva 2016/680 relativa à proteção de dados em matéria penal, permitindo a transferência de dados pessoais do Espaço Económico Europeu (EEE) para o Reino Unido.. As duas decisões incluíam uma cláusula de caducidade definida para 27 de junho de 2025, salvo renovação. Em outubro de 2024, o governo do Reino Unido apresentou o projeto de lei *Data (Use and Access) Bill*, que propõe alterar certos aspetos da legislação de proteção de dados do Reino Unido.

Como não era esperado que o processo legislativo estivesse concluído antes da primavera de 2025, a Comissão propôs uma prorrogação técnica limitada de seis meses, até 27 de dezembro de 2025, para permitir a conclusão do processo legislativo, mantendo a proteção adequada dos dados. A Comissão solicitou o parecer da Autoridade Europeia para a Proteção de Dados (AEPD), que considerou a prorrogação razoável, salientando a sua natureza excecional e a necessidade de avaliar o quadro jurídico final depois de adotado. A AEPD esclareceu que esta prorrogação não reabre nem modifica as suas avaliações anteriores sobre a adequação do Reino Unido — que serão avaliadas após a conclusão do processo legislativo — nem prejudica decisões futuras, e que os seus pareceres emitidos em 2021 (Pareceres 14/2021 e 15/2021) permanecem válidos e devem ser tidos em conta em avaliações futuras.

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

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

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

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

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

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

Laia Llambric
Associada - Bilbau
laia.llambrich@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: