GARRIGUES

Newsletter Economia de Dados, Privacidade e Cibersegurança

Abril 2025

Índice

1. A Comissão Europeia continua a desvendar o Regulamento de Inteligência Artificial: definição de um sistema de inteligência artificial e código de boas práticas para IA de finalidade geral

No dia 6 de fevereiro, a Comissão Europeia publicou as orientações para ajudar os diversos operadores no ambiente de inteligência artificial a analisar se estão perante um sistema de inteligência artificial nos termos do Regulamento (UE) 2024/1689 sobre Inteligência Artificial. Além disso, em 11 de março, publicou o terceiro projeto do Código de Boas Práticas para a IA de finalidade geral. No artigo seguinte, detalhamos os pontos principais de ambos os documentos.

Alejandro Padín Vidal

No passado dia 6 de fevereiro, no cumprimento do disposto na alínea f) do n.º 1 do artigo 96.º do Regulamento IA, a Comissão Europeia publicou as **orientações sobre a definição de sistemas de inteligência artificial**, que se juntam às publicadas 2 dias antes sobre as práticas proibidas de inteligência artificial, sobre as quais já publicamos anteriormente este post.

Estas novas orientações destinam-se a ajudar os operadores a identificar se estão perante um sistema de inteligência artificial regulado pelo Regulamento de IA.

As orientações procuram especificar a definição de "**sistema de inteligência artificial**" contida no n.º 1 do artigo 3.º do Regulamento de IA. Como se pode observar neste artigo, e conforme resulta das orientações, ao analisar se estamos perante um sistema de inteligência artificial, devemos encontrar um sistema que cumpra todos estes requisitos:

i. **Baseado numa máquina** (*hardware* e *software*).

ii. Concebido para **funcionar com diferentes níveis de autonomia**, ou seja, que possa atuar com um certo grau de independência da ação humana e tenha determinadas capacidades para funcionar sem intervenção humana.

iii. Que possa demonstrar **capacidade de adaptação após a implementação**, elemento que não é um requisito essencial para estar no âmbito do Regulamento IA. Ou seja, um sistema de inteligência artificial pode ser considerado como tal para efeitos do Regulamento IA, mesmo que não tenha capacidade de adaptação após a implementação.

iv. Que tenha **objetivos explícitos ou implícitos**, ou seja, objetivos claramente declarados que sejam codificados diretamente pelo desenvolvedor do sistema (por exemplo, otimização de

custos numa função) e objetivos que não sejam explicitamente declarados, mas podem ser inferidos a partir do comportamento subjacente ou das presunções subjacentes do sistema.

v. **Que infira** da informação de entrada que recebe **o modo de gerar resultados de saída**, ou seja, não depende de regras predefinidas por humanos para executar operações automaticamente.

   As orientações citam alguns exemplos que não cumpririam este requisito e, por conseguinte, não seriam considerados um sistema de inteligência artificial para efeitos do Regulamento de IA: sistemas de gestão de bases de dados para filtragem ou seleção de acordo com determinados critérios ou sistemas de análise puramente descritiva, como um *software* que utiliza técnicas estatísticas sobre dados de inquéritos.

vi. Os resultados gerados podem incluir, entre outros, **previsões, conteúdo, recomendações ou decisões**. O Regulamento IA utiliza a expressão "como", o que significa que o resultado de saída pode ser outro.

vii. Que o resultado de saída possa **influenciar ambientes físicos ou virtuais**. A própria redação do regulamento determina que esta influência não é essencial para a qualificação de um sistema como IA.

Embora estas orientações ainda não tenham sido formalmente aprovadas e não sejam vinculativas, podem ajudar a interpretar alguns dos muitos termos vagos contidos no artigo 3.º do Regulamento de IA. Isto pode ser especialmente útil tendo em conta que a maioria das empresas está a correr contra o tempo para rever e classificar os sistemas de inteligência artificial que utilizam, desenvolvem ou introduzem no mercado.

IA de finalidade geral

O outro documento publicado pela Comissão Europeia a que nos referimos é o terceiro projeto do Código de Boas Práticas para a Inteligência Artificial (IA) de Finalidade Geral, elaborado por peritos independentes. Este documento é essencial para detalhar as obrigações estabelecidas no **Regulamento de IA**, fornecendo aos fornecedores orientações claras para garantir a conformidade regulamentar e promover o desenvolvimento de modelos de IA seguros e fiáveis.

Este terceiro projeto apresenta uma estrutura mais simplificada e precisa em comparação com as versões anteriores. Centra-se numa série de compromissos de alto nível, acompanhados de medidas detalhadas para a sua implementação eficaz. Entre os aspetos que merecem destaque, incluem-se:

- **Transparência e direitos de autor**: todos os fornecedores de modelos de IA de finalidade geral devem cumprir obrigações específicas em matéria de transparência e direitos de autor. Para facilitar este processo, foi introduzido um formulário de documentação normalizado que permite que as informações necessárias sejam recolhidas e apresentadas de forma consistente e acessível.

- **Avaliação e mitigação de riscos sistémicos**: para os fornecedores de modelos de IA que possam representar riscos sistémicos (conforme se definem no Regulamento de IA), o Código estabelece medidas específicas. Entre elas estão a realização de avaliações abrangentes dos modelos, a implementação de estratégias de mitigação de riscos, a notificação obrigatória de incidentes graves e o cumprimento de normas rigorosas de cibersegurança.

A criação deste código foi um esforço colaborativo, coordenado pelo **Gabinete Europeu de IA**, com a participação ativa de quase 1000 partes interessadas, incluindo fornecedores de modelos de IA, intermediários, representantes da indústria, da sociedade civil, académicos e especialistas independentes. Esta diversidade garante que o código reflete uma vasta gama de perspetivas e conhecimentos especializados.

Para os profissionais do direito especializados no mundo digital, este código representa uma ferramenta essencial. Fornece uma estrutura detalhada sobre as responsabilidades e as melhores práticas para os fornecedores de modelos de IA de finalidade geral, facilitando a interpretação e a aplicação do Regulamento de IA. Além disso, promove a adoção de práticas que equilibrem a inovação tecnológica com a proteção dos direitos fundamentais e a segurança dos utilizadores.

Prevê-se que o código final esteja pronto até maio de 2025, fornecendo aos prestadores orientações claras para demonstrar o cumprimento do Regulamento de IA antes da sua aplicação plena em agosto de 2025. A versão final integrará os contributos recebidos durante esta fase final de consulta, garantindo que as orientações são práticas e adaptadas às necessidades do setor.

Próximos passos

A complexidade jurídica e técnica desta nova norma exige análise e adaptação por parte de todos os envolvidos no desenvolvimento de tecnologia e conformidade regulamentar. Isto é demonstrado pelo facto de a própria Comissão Europeia estar a publicar materiais para auxiliar na interpretação e aplicação da norma.

2. Resoluções das autoridades de proteção de dados

A Agência Espanhola de Proteção de Dados (AEPD) sanciona uma seguradora em 5 milhões de euros por exfiltrar dados de milhões de clientes

Em setembro de 2022, uma seguradora sofreu um ataque de força bruta ao seu formulário de consulta de clientes utilizando as credenciais de um dos seus mediadores. Posteriormente, os dados pessoais de mais de 1,6 milhões de clientes e ex-clientes foram expostos a acesso não autorizado, incluindo o nome completo, número de identidade, número de telefone, morada completa, estado civil, data e país de nascimento, e até mesmo os IBAN das contas bancárias.

Na sua resolução PS-00453-2023**,** a AEPD determinou que a entidade violou os artigos 5.º, n. 1, al. f), 25.º, 32.º e 35.º do RGPD na medida em que (i) não garantiu a segurança adequada dos dados pessoais, incluindo tanto o tratamento não autorizado ou ilícito resultante do ciberataque como a visualização e acesso aos dados de antigos clientes por parte dos mediadores de seguros no momento do incidente; (ii) independentemente da violação, as medidas de segurança que implementou foram insuficientes; (iii) aquando da conceção da aplicação ou sistema em causa, não teve adequadamente em conta os princípios de minimização e limitação de dados; e (iv) tendo em conta o volume de dados tratados (incluindo categorias especiais) e os riscos de apropriação indevida dos dados por terceiros, deveria ter realizado uma avaliação de impacto sobre a proteção de dados. Por todos estes motivos, a seguradora foi sancionada em 5 milhões de euros.

Uma plataforma de *streaming* é sancionada em 4,75 milhões de euros por não fornecer informações adequadas sobre o tratamento

A investigação teve início em 2019 após duas queixas apresentadas pela Noyb (uma ONG austríaca focada na privacidade) em nome de dois titulares de dados à Autoridade Austríaca de Proteção de Dados (Datenschutzbehörde) e posteriormente encaminhadas para a Autoridade Holandesa de Proteção de Dados (Autoriteit Persoonsgegevens), que confirmou que a entidade denunciada tinha cometido várias infrações do RGPD.

Mais especificamente, na resolução de 18 de dezembro de 2024 constatou-se uma violação do artigo 12.º, n.º 1, em relação com o artigo 13.º, n.º 1 e 2 do RGPD entre 25 de maio de 2018 e 30 de julho de 2020, devido à falta de informação sobre as finalidades e bases de legitimação do tratamento, os destinatários dos dados, os períodos de conservação e as garantias utilizadas no caso de transferências internacionais de dados para fora do Espaço Económico Europeu na sua política de privacidade. Além disso, a empresa não atendeu adequadamente aos pedidos de

acesso enviados, violando assim o artigo 12.º, n.º 1, em conjunto com o artigo 15.º, n.º 1 e 2, do RGPD entre 25 de outubro de 2018 e 19 de novembro de 2020, porque, entre outras coisas, não forneceu informações específicas sobre os dados pessoais utilizados e os seus destinatários.

A autoridade polaca de controlo de proteção de dados aplicou uma coima de 928.498,06 euros a um banco por não ter informado os seus clientes sobre uma violação de dados pessoais

Um funcionário do banco enviou por engano documentos pertencentes aos clientes da requerida para outro banco, em que se encontravam informações pessoais (nome e apelido, nome dos pais, contas bancárias, moradas, rendimentos, etc.). A autoridade de controlo instou a entidade a informar os clientes afetados pela violação, mas a requerida não o fez, argumentando que o terceiro que teve acesso aos dados era também uma instituição bancária e, por isso, estava sujeita ao sigilo bancário, tornando-se, assim, uma *trusted entity*.

A autoridade de controlo afirma na sua resolução que não é o estatuto do terceiro que determina se este é de confiança, mas sim a existência de uma relação direta (e permanente) entre o remetente e o destinatário. Neste caso, não existe tal relação entre as entidades bancárias, pelo que não é possível garantir que o terceiro era de confiança. Consequentemente, a violação deveria ter sido comunicada aos titulares. Por este motivo, a autoridade de controlo aplicou uma coima de 928.498,06 € à entidade por violação do artigo 34.º do RGPD.

A CNIL aplica uma coima de 40.000 euros a uma empresa imobiliária por vigilância excessiva dos seus funcionários

A empresa tinha instalado um software de monitorização das atividades dos colaboradores para os dias de teletrabalho para medir o tempo de trabalho efetivo e a produtividade dos colaboradores. Instalou também câmaras de videovigilância que captavam continuamente imagens e sons dos trabalhadores, tanto nas áreas de trabalho como de descanso.

Na sua resolução a CNIL considera que a empresa não demonstrou motivos suficientes para exercer esse nível de vigilância sobre os seus colaboradores e, por isso, considera tal tratamento excessivo. Além disso, no âmbito da investigação, a CNIL determinou também que a empresa não informou adequadamente os funcionários sobre estas operações de tratamento, nem conduziu uma avaliação de impacto ou implementou medidas de segurança adequadas para estes tratamentos. Por isso, impõe uma coima de 40.000 euros à empresa por violação dos artigos 6.º, 12.º, 13.º, 32.º e 35.º do RGPD.

Uma empresa de telecomunicações é sancionada com duas coimas por violar os artigos 5.º, n.º 1, alínea f) e 32.º do RGPD devido a uma falha de segurança

Em 26 de setembro de 2022, a empresa de telecomunicações em causa notificou a AEPD sobre uma violação de segurança causada pelo acesso não autorizado de terceiros aos dados pessoais tratados pela empresa na sua qualidade de responsável, afetando mais de um milhão de clientes. Na sequência desta notificação, foi iniciada uma investigação preliminar para apurar se a entidade tinha violado as normas, determinando-se, em última instância, que comunicasse a violação aos titulares dos dados afetados. Embora a empresa se tenha oposto inicialmente à ordem, alegando que os afetados pelo incidente não eram identificáveis, após uma série de pedidos de informação, a entidade acabou por efetuar essa comunicação.

Como resultado, a AEPD decidiu iniciar um processo sancionador contra a empresa pela alegada violação dos artigos 5.º, n.º 1, al. f) (relativo aos princípios de integridade e confidencialidade) e 32.º (relativo às medidas de segurança) do RGPD, conforme o

tipificado nos números 4 e 5 do artigo 83.º do RGPD, respetivamente. Por fim, propõe uma coima total de 1.300.000 euros pela prática das referidas violações.

Na resolução do processo sancionador, a AEPD confirma a sanção proposta, enfatizando as seguintes questões:

1. Em relação à **natureza dos dados afetados**, recorde-se que, atualmente, um número de telefone — seja fixo ou móvel — se enquadra perfeitamente na definição de dados pessoais do artigo 4.º, n.º 1 do RGPD. Por um lado, permite, por si só, identificar a pessoa a quem pertence, mesmo quando não é acompanhado de quaisquer outros dados. Por outro lado, é possível identificar a pessoa a quem pertence o número de telefone sem fazer esforços desproporcionados.

   Acrescenta ainda que, neste caso, as informações recolhidas pelos atacantes (o endereço MAC -*Media Access Control*- e os dados do fabricante do dispositivo, a configuração da porta de ligação associada ao telefone fixo, os nomes da rede Wi-Fi e a sua palavra-passe, etc.) devem também ser consideradas dados pessoais, uma vez que se trata de informação relativa a pessoas singulares identificadas ou identificáveis, já que, com os dados afetados pela violação, é possível identificar os titulares das mesmas sem esforço exagerado ou desproporcional.

2. Por outro lado, **a AEPD defende que a conduta da empresa sancionada se enquadra perfeitamente nas violações citadas**, uma vez que o processo demonstra que a entidade não dispunha de medidas adequadas para garantir um nível de segurança adequado ao risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares.

3. Quanto à **falta de diligência** da empresa, a AEPD considera que é evidente, uma vez que a entidade não dispunha de medidas adequadas de controlo de acesso à aplicação para colaboradores que estava publicada online, nem dispunha de medidas destinadas a gerar alertas e bloqueios em caso de situações completamente anómalas, não tendo sido gerados quaisquer alertas ou eventos de segurança com aviso imediato ao CSIRT-TE (Equipa de Resposta perante Incidentes de Segurança da entidade).

4. Por fim, a AEPD também não acredita que haja qualquer **ausência de culpabilidade**, pois entende que as medidas que deveriam ter sido aplicadas à data do sucedido eram conhecidas de acordo com o estado da técnica e tinham um custo acessível.

Duas sociedades sancionadas por publicar na internet imagens de menores sem o seu consentimento

No primeiro caso, a entidade demandada publicou no seu site uma imagem da demandante, menor de idade, obtida através de um terceiro - Telegram - como acompanhamento de uma notícia relativa ao pai da menor, figura pública. No segundo caso, a entidade demandada publicou no seu canal de Telegram uma imagem da demandante, menor de idade, captada num espaço público e inserida num chat em que se lançaram diversos insultos sobre a sua pessoa.

Em ambos os casos, a AEPD conclui que o tratamento realizado pelas requeridas é excessivo, uma vez que a divulgação das imagens dos menores era desnecessária para a finalidade de informação que se pudesse considerar legítima. Consequentemente, considera que os factos constituem uma violação do artigo 5.º, n.º 1, al. c) do RGPD.

De igual modo, considera adequado graduar as sanções em função (i) da natureza, gravidade e duração das violações, uma vez que a publicação das imagens, em ambos os

casos, foi realizada através de canais que permitiram a divulgação imediata e ampla dos conteúdos publicados; (ii) da intencionalidade, uma vez que a publicação foi feita diretamente pelas requeridas; e (iii) do impacto nos direitos dos menores. Por tudo isto, em ambos os casos foi aplicada uma coima administrativa de 5000 euros, assim como a medida definitiva de remoção dos conteúdos publicados no canal correspondente.

A autoridade finlandesa de controlo aplicou uma coima de 2,4 milhões de euros a uma empresa de serviços postais por incumprimento dos artigos 5.º e 6.º, n.º 1 do RGPD

Neste caso, a entidade, o principal serviço postal do país, tinha criado uma caixa de correio eletrónico automatizada para comunicar com os seus clientes sem a sua autorização e, muitas vezes, sem o seu conhecimento, substituindo a correspondência postal tradicional. Além disso, a caixa de correio estava ligada a um conjunto mais vasto de serviços, sem permitir ao cliente escolher se a queria ou não utilizar, uma vez que os diferentes serviços estavam ligados entre eles num único contrato. Deste modo, a caixa de correio eletrónico não poderia ser dispensada sem que os outros serviços também cessassem.

A autoridade finlandesa considera que o serviço solicitado pelo cliente poderia ter sido prestado sem a criação automática de uma caixa de correio eletrónico. Além disso, considera que o responsável pelo tratamento também não informou adequadamente os seus clientes sobre a ativação dessa caixa de correio, além de uma série de definições técnicas no serviço que não estavam em conformidade com os requisitos impostos pelas normas de proteção de dados aplicáveis (por exemplo, foi incluída uma função de seleção ativada automaticamente, assim como uma caixa de seleção pré-marcada).

O procedimento sancionatório culmina com a aplicação de uma coima de 2,4 milhões de euros ao responsável, ordenando ainda à entidade a adoção de um conjunto de medidas corretivas.

De acordo com a AEPD, a utilização de modelos biométricos encriptados para controlo de presenças constitui um tratamento de dados biométricos

A Agência Espanhola de Proteção de Dados (AEPD) sancionou uma associação profissional em 20.000 euros por utilizar um sistema de controlo de assiduidade por impressão digital, implementado antes da publicação do Guia da AEPD sobre o tratamento do controlo de assiduidade através de sistemas biométricos. O sistema não obteve o levantamento da proibição do tratamento de dados biométricos e não dispunha de uma avaliação de impacto adequada ao tratamento.

A Autoridade considera os modelos biométricos encriptados como categorias especiais de dados pessoais, cujo tratamento é proibido, a menos que se aplique uma das exceções previstas no artigo 9.º, n.º 2 do RGPD. Para levantar a proibição, a associação argumentou que a utilização do sistema estava protegida pelas obrigações legais do Estatuto dos Trabalhadores para o controlo do trabalho. A AEPD contra-argumenta que regulamentação não exige o uso de biometria e que as exceções devem ser interpretadas de forma restritiva.

Embora a associação tenha apresentado uma Avaliação de Impacto de Proteção de Dados (DPIA), a AEPD avaliou o seu conteúdo, concluindo que o sistema não era funcional, necessário ou proporcional, especialmente porque já estavam em vigor métodos alternativos, como os códigos alfanuméricos.

A CNIL impõe uma coima de 50 milhões de euros a uma operadora telefónica por exibir publicidade encoberta sem o devido consentimento

A Autoridade Francesa de Proteção de Dados (CNIL) aplicou uma coima de 50 milhões de euros a uma operadora telefónica por inserir publicidade sem o devido consentimento nas caixas de entrada dos utilizadores das contas de correio eletrónico da operadora, em violação do artigo 34.º, n.º 5 do Código francês das Comunicações Postais e Eletrónicas (que é equivalente em Espanha ao artigo 21.º da Lei dos Serviços da Sociedade da Informação).

A CNIL observou que a empresa detinha controlo sobre os anúncios em causa, uma vez que geria e comercializava os espaços dedicados aos anunciantes nas caixas de entrada dos utilizadores. A autoridade considerou ainda, no entanto, que foram tomadas medidas corretivas ao cessar a utilização deste tipo de publicidade em novembro de 2023, após a implementação de um novo sistema de publicidade que permite uma distinção clara entre anúncios e mensagens de correio eletrónico legítimas.

Além disso, a autoridade identificou uma violação do artigo 82.º da Lei de Proteção de Dados francesa relativamente à utilização de cookies, pois concluiu que, apesar da retirada do consentimento do titular dos dados, as informações continuaram a ser recolhidas através dos mesmos.

Dupla penalização em matéria de videovigilância pela instalação de um sistema que capta imagens em espaços públicos sem autorização administrativa e sem inclusão da informação exigida

Foi apresentada uma reclamação relativa à instalação de um sistema de videovigilância, existindo indícios de uma eventual violação das normas de proteção de dados pessoais. A reclamação baseia-se no facto de a requerida ter instalado uma câmara de videovigilância capaz de captar imagens da via pública, sem ter obtido a prévia autorização administrativa.

A resolução PS-00399-2023 da AEPD sanciona a requerida, uma vez que, de facto, existia uma câmara de videovigilância capaz de captar imagens da via pública. Além disso, embora a câmara estivesse assinalada com uma placa que indicava uma área de videovigilância, essa placa não fazia referência à atual regulamentação de proteção de dados pessoais, nem incluía as informações necessárias sobre o responsável pelo tratamento de dados ou o endereço onde os titulares dos dados se deveriam dirigir para exercer os seus direitos.

Segundo a AEPD, os factos configuram uma dupla infração, imputável à requerida, por violação dos artigos 5.º, n.º 1, al. c) (minimização de dados) e 13.º (informação a prestar ao titular dos dados) do RGPD, fixando-se para cada uma delas uma coima de 500 euros.

Um meio de comunicação social foi sancionado em 10 mil euros por publicar o nome de uma pessoa singular

Na sua resolução PS-00335-2023, a AEPD aplicou uma sanção a um conhecido meio de comunicação social por publicar no seu site uma notícia sobre a divulgação de um vídeo nas redes sociais, em que incluía o nome e a imagem da parte reclamante, assim como links para o vídeo objeto da reclamação.

No entender da AEPD, a inclusão em publicações jornalísticas de uma imagem de uma pessoa ou de um vídeo que contenha a sua imagem e voz de forma que seja identificada ou identificável — neste caso, em conjunto com o seu nome — constitui tratamento de dados pessoais, devendo ser conciliado o direito à informação e o direito à proteção de dados. No caso em apreço, a AEPD considera que o meio de comunicação tratou dados excessivos, por não serem necessários para a finalidade pretendida.

Assim, a entidade é sancionada em 10.000 euros pela violação do artigo 5.º, n. 1, al. c) do RGPD, tipificada no artigo 83.º, n.º 5 do mesmo regulamento e classificada como muito grave para efeitos de prescrição.

A Autoridade Italiana de Proteção de Dados (IDPA) sanciona a OpenAI em 15 milhões de euros por recolher dados pessoais para treinar o ChatGPT

Em março de 2023, a Itália tornou-se o primeiro país ocidental a bloquear temporariamente o ChatGPT por motivos de privacidade, depois de a Autoridade Italiana de Proteção de Dados (IDPA) ter anunciado uma investigação sobre alegadas violações das regras de proteção de dados.

Como resultado destas investigações, a autoridade identificou potenciais violações devido à falta de transparência da OpenAI em relação à origem dos dados utilizados para treinar o ChatGPT - mais especificamente os dados pessoais correspondentes a cidadãos italianos -, assim como uma violação de segurança que terá ocorrido em março de 2023 e sobre a qual a empresa não tinha informado as autoridades. Tudo isto levou à imposição de uma coima de 15 milhões de euros à OpenAI e à obrigação de explicar ao público como funciona o ChatGPT, principalmente no que diz respeito à recolha de dados para treino do modelo.

O regulador observa na sua decisão que a OpenAI também "tratou dados pessoais dos utilizadores" para treinar o chatbot sem primeiro identificar uma "base legal apropriada" para a ação, violando o "princípio de transparência e as obrigações de informação relacionadas com os utilizadores." Além disso, segundo a agência, a OpenAI não disponibilizou mecanismos de verificação da idade, o que traz o risco de expor as crianças com menos de 13 anos a respostas inadequadas ao seu nível de desenvolvimento e autoconhecimento.

Por fim, considerando que a empresa estabeleceu a sua sede europeia na Irlanda durante a investigação, a autoridade italiana remeteu os documentos processuais para a Autoridade Irlandesa de Proteção de Dados (DPC), que se tornou a principal autoridade de controlo ao abrigo do RGPD, para que esta possa retomar a investigação sobre possíveis violações de forma continuada.

Foi mantida uma coima de 200.000 euros para uma empresa de telecomunicações por duplicar cartões SIM a pedido de um terceiro que não o titular da linha

A AEPD confirmou a coima de 200.000 euros imposta a uma empresa de telecomunicações por produzir um duplicado do cartão SIM da linha telefónica da parte reclamante. A empresa indicou que a segunda via do cartão SIM foi solicitada por um terceiro que conhecia as informações pessoais do reclamante e, embora os protocolos de segurança tenham sido seguidos, um único erro permitiu o tratamento fraudulento. Além disso, bloqueou o SIM no dia seguinte e devolveu os valores afetados.

A empresa alegou que tinha tomado as medidas técnicas e organizacionais adequadas para identificar clientes e evitar fraudes de duplicação de cartões SIM; que a duplicação de um cartão SIM não permite o acesso direto a informações bancárias, palavras-passe ou outros dados confidenciais; e implementou medidas de segurança diligentes.

Contudo, a AEPD respondeu que não avalia a adequação das medidas, mas sim o seu incumprimento neste caso concreto, o que viola o artigo 6.º, n.º 1 do RGPD; que o SIM duplicado não dá acesso direto à informação bancária, mas é um elemento necessário para a prática de fraudes; que a negligência da Vodafone é evidente na falta de controlo e supervisão dos seus agentes; e que a empresa não pode fugir à sua responsabilidade alegando fatores externos

O proprietário de uma casa de férias foi sancionado por recolher indevidamente fotos dos documentos de identidade dos hóspedes

A 18 de outubro de 2024, a Agência Espanhola de Proteção de Dados (AEPD) iniciou um processo sancionatório contra o proprietário de uma casa de férias após uma queixa que alegava a recolha indevida de imagens dos documentos de identificação dos hóspedes como parte do processo de *check-in* online. Este tratamento excedia o que era necessário segundo os regulamentos de proteção de dados, violando o princípio de minimização de dados do Artigo 5.º, n.º 1, al. c) do RGPD.

O processo foi concluído depois de o requerido ter reconhecido a responsabilidade e efetuado um pagamento voluntário de 600 € em 11 de novembro de 2024. A AEPD ordenou ainda que os procedimentos sejam colocados em conformidade com os regulamentos e que quaisquer dados pessoais excedentes armazenados sejam eliminados, concedendo um prazo de dois meses para o seu cumprimento.

A Agência Espanhola de Proteção de Dados reafirma com esta decisão a necessidade de os responsáveis pelo tratamento adotarem práticas proporcionais e adequadas no tratamento de dados pessoais, especialmente nas atividades relacionadas com o alojamento e os serviços digitais.

Uma empresa de embalagens de cartão foi sancionada por duas violações do RGPD

A Agência Espanhola de Proteção de Dados (AEPD) decidiu impôr sanções a uma empresa de embalagens de cartão após ter identificado duas violações do Regulamento Geral de Proteção de Dados (RGPD).

A primeira violação, relacionada com o artigo 35.º, foi classificada como grave e sancionada com 200.000 euros devido à ausência de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD). A entidade utilizou um sistema de reconhecimento facial para controlar o horário dos seus 99 colaboradores sem ter realizado a AIPD obrigatória, uma medida essencial para avaliar riscos inerentes aos dados biométricos, que são considerados uma categoria especial pelo RGPD. A empresa continuou a utilizar o sistema durante anos sem fazer as adaptações necessárias depois de o RGPD ter entrado em vigor em 2018, o que agravou a sua responsabilidade.

A segunda violação, punida com uma coima de 20.000 euros, corresponde a uma violação do artigo 15.º do RGPD, por não acolher adequadamente o direito de acesso do trabalhador. Apesar dos pedidos do titular, a denunciada não prestou informações completas nem as prestou no prazo estabelecido, incumprindo, assim, as suas obrigações legais. A AEPD determinou ainda que a entidade adote medidas corretivas, incluindo a garantia do cumprimento do direito de acesso e a adequação dos seus procedimentos ao RGPD para evitar futuras violações.

Um clube desportivo é sancionado em 200.000 euros por violação do artigo 5.º, n.º 1, al. c) do RGPD através da instalação de um sistema de reconhecimento facial para acesso ao seu estádio

A 22 de novembro de 2022, a AEPD recebeu uma queixa contra um clube desportivo por implementar um sistema de reconhecimento facial biométrico para acesso ao seu estádio. Este sistema, implementado em abril de 2022, foi apresentado pelo clube aos sócios como ocasional e complementar aos métodos de acesso existentes (ou seja, cartão físico, cartão digital no telemóvel e código QR). A denúncia alegava que o sistema restringia as liberdades e os direitos fundamentais e que a sua falta de proporcionalidade significava que mesmo o consentimento dos titulares dos dados era insuficiente para legitimar o tratamento dos dados.

A 14 de dezembro de 2023, a AEPD decidiu iniciar um processo sancionatório contra o clube pela alegada violação dos artigos 5.º, n.º 1, al. c) (minimização de dados) e 9.º do RGPD (tratamento de categorias especiais de dados pessoais), ambas tipificadas no artigo 83.º, n.º 5, al. a) do RGPD. Além disso, determinou, como medida provisória, a suspensão temporária de todo o tratamento de dados pessoais relativos à solução de reconhecimento facial para acesso ao estádio. Por fim, propõe uma coima de 200.000 euros pela prática de cada uma das referidas violações.

Na sua decisão do processo sancionatório, a AEPD confirma a sanção imposta quanto à violação do artigo 5.º, n.º 1, al. c) do RGPD, e determina tanto a proibição definitiva do tratamento de dados através de reconhecimento facial como a eliminação de quaisquer registos onde tenham sido armazenados dados biométricos, destacando as seguintes questões:

1. O tratamento de dados pessoais deve obedecer aos **princípios estabelecidos no artigo 5.º do RGPD**, que incluem a licitude, a lealdade, a transparência, a limitação da finalidade, a minimização de dados, a exatidão, a limitação do período de conservação, a integridade e confidencialidade e a responsabilização proativa. Estes princípios garantem que os dados são tratados adequadamente e com respeito pelos direitos dos respetivos titulares. A AEPD sublinha na sua resolução que o tratamento de dados biométricos pelo clube não vai ao encontro destes princípios, especialmente no que diz respeito à minimização de dados.

2. Quanto à **necessidade e proporcionalidade do tratamento**, a AEPD conclui que o tratamento dos dados biométricos através do sistema de reconhecimento facial não cumpriu os critérios de necessidade e proporcionalidade acima referidos. Avaliar a necessidade implica determinar se o tratamento é essencial para atingir a finalidade perseguida e se não existem outros meios menos invasivos de atingir o mesmo objetivo. Neste caso, a AEPD determinou que existiam métodos menos invasivos, como a utilização de cartões físicos ou digitais, que poderiam atingir os mesmos objetivos sem a necessidade de tratar dados biométricos.

3. Além disso, a AEPD sublinha na sua resolução que o tratamento de dados biométricos pelo clube não reuniu as condições necessárias para levantar a proibição do tratamento de **categorias especiais de dados**, uma vez que não foi demonstrado que o consentimento explícito dos assinantes fosse suficiente para justificar o tratamento em termos de necessidade e proporcionalidade.

Contudo, a AEPD não avalia o incumprimento do artigo 9.º do RGPD, pois considera que, uma vez que o tratamento não passou no teste da necessidade e da proporcionalidade, não deve avaliar a legitimidade da sua base jurídica.

Uma entidade corretora de valores mobiliários é instada a cumprir o direito de acesso solicitado pela parte reclamante.

A parte reclamante apresentou uma reclamação contra uma corretora de valores mobiliários porque, após exercer o direito de acesso aos seus dados pessoais perante a referida entidade, esta respondeu que era considerada um sujeito obrigado de acordo com o disposto no artigo 2.º, n.º 1, al. i) da Lei 10/2010, de 28 de abril, relativa à prevenção do branqueamento de capitais e do financiamento do terrorismo (LPBCFT) e que, de acordo com o artigo 32.º, n.º 2 da referida lei, estes sujeitos não estavam obrigados a satisfazer os direitos estabelecidos nos artigos 15.º a 22.º do RGPD.

A este propósito, na sua decisão a AEPD alega que a parte requerida apenas transcreve o artigo 32.º da LPBCFT na sua resposta, mas não comprova ter enviado a informação necessária sobre os dados não sujeitos à limitação, ou seja, a confirmação de

que os seus dados estão ou não a ser tratados, o acesso efetivo aos mesmos e o acesso à informação sobre o tratamento, de acordo com o artigo 13.º do RGPD. Ou seja, a excepção do artigo 32.º da LPBCFT não permite que o pedido seja ignorado como se não tivesse sido formulado, não lhe dando resposta, pelo que se condena a entidade a prestar as referidas informações.

A autoridade catalã de proteção de dados sancionou um prestador de cuidados de saúde em 30.000 euros por aceder a um registo clínico

A Autoridade de Proteção de Dados da Catalunha sancionou uma entidade de serviços de saúde de gestão pública em 30.000 euros por aceder aos registos clínicos de uma pessoa sem o seu consentimento em nove ocasiões. No entanto, a coima foi reduzida para 24.000 euros depois de o requerido ter admitido a responsabilidade, o que representa uma redução de 20%.

O incidente ocorreu entre maio e julho de 2023, quando um profissional da organização acedeu indevidamente aos registos clínicos de uma mulher em nove ocasiões. Os acessos não estavam relacionados com qualquer atendimento ou intervenção de diagnóstico, pois a pessoa afetada nunca tinha sido vista por este profissional nem tinha sido doente daquele centro, pelo que não existia qualquer relação entre eles. A reclamante descobriu o que tinha acontecido quando solicitou um relatório detalhado de acesso ao seu histórico.

Por tudo isto, a Autoridade de Proteção de Dados da Catalunha considera que a organização pública violou o artigo 5.º, n.º 1, al. f) do RGPD (princípio de integridade e confidencialidade).

O Tribunal Geral da UE reafirma a capacidade do CEPD de exigir investigações adicionais quando as decisões preliminares de uma autoridade de controlo principal não abordam adequadamente os aspetos relevantes de um caso

O caso surgiu de um litígio entre a Comissão de Proteção de Dados da Irlanda (DPC) e o Comité Europeu para a Proteção de Dados (CEPD). A Autoridade Irlandesa, atuando como autoridade de controlo principal, emitiu decisões preliminares sobre o tratamento de dados pelo Facebook, Instagram e WhatsApp. No entanto, outras autoridades de controlo discordaram destas decisões e apresentaram oposições relevantes e fundamentadas, levando a Autoridade Irlandesa a remeter o assunto para o CEPD para resolução de litígios ao abrigo do mecanismo de consistência do RGPD.

Nas decisões vinculativas do CEPD de dezembro de 2022, o CEPD instruiu a Autoridade Irlandesa para ampliar a sua investigação e emitir novas decisões preliminares. A DPC contestou estas decisões perante o Tribunal Geral, argumentando que o CEPD tinha excedido a sua competência. No entanto, no seu acórdão de 29 de janeiro de 2025, nos processos apensos T-70/23 y T-84/23, o Tribunal Geral rejeitou as ações da Autoridade Irlandesa e confirmou a competência do CEPD para exigir uma nova investigação e a emissão de novas decisões preliminares.

A exceção à obrigação de informar o titular dos dados aplica-se a todos os dados pessoais que o responsável pelo tratamento não tenha obtido diretamente

O Supremo Tribunal da Hungria requereu uma decisão preliminar relativa à interpretação dos artigos 14.º, n.º 1 e 5, alínea c), 32.º e 77.º, n.º 1, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

No âmbito da emissão de um certificado de vacinação contra a COVID-19, um titular de dados apresentou uma reclamação contra a administração húngara responsável pela emissão do certificado, alegando que esta não cumpriu o seu dever de prestar informações.

A autoridade emissora do certificado indica que não é obrigada a fornecer informações sobre o tratamento de dados pessoais, uma vez que, de acordo com o artigo 14.º, n.º 5, al. c) do RGPD, a recolha de dados pessoais está prevista pela legislação nacional húngara e, consequentemente, os dados (i) foram obtidos através de outro organismo da administração e (ii) foram gerados pela autoridade emissora no exercício das suas funções.

O tribunal húngaro competente declarou no seu acórdão que a exceção do artigo 14.º, n.º 5 do RGPD não é aplicável neste caso, uma vez que no contexto dos certificados de imunidade são gerados dados que o responsável pelo tratamento não obtém de outros organismos, mas antes produz ele próprio no exercício das suas funções (como, por exemplo, o código QR integrado no cartão).

No processo de recurso, o Supremo Tribunal Húngaro suspendeu o processo e perguntou ao TJUE se o artigo 14.º, n.º 5, al. c) do RGPD deveria ser interpretado no sentido de que a exceção à obrigação do responsável pelo tratamento de informar o titular dos dados se aplica apenas aos dados pessoais obtidos de terceiros, ou se se estende também aos dados pessoais gerados pelo próprio responsável pelo tratamento no exercício das suas funções.

No seu acórdão de 28 de novembro de 2024, processo C-169/2023, o TJUE responde que o artigo 14.º, n.º 5, al. c) do RGPD deve ser interpretado no sentido de que a exceção à obrigação de fornecer informações ao titular dos dados pelo responsável pelo tratamento afeta indistintamente todos os dados pessoais que o responsável pelo tratamento não obteve diretamente do titular, tenham sido obtidos pelo responsável pelo tratamento de uma pessoa diferente do titular, ou gerados pelo próprio responsável pelo tratamento no exercício das suas funções.

O Supremo Tribunal admite um recurso sobre os deveres de transparência da Administração Pública na utilização de programas informáticos

No seu despacho de 14188/2024, o Supremo Tribunal admitiu o recurso interposto de uma decisão da Audiência Nacional que manteve a recusa do Ministério da Transição Ecológica em fornecer o código do BOSCO, aplicação desenvolvida para decidir sobre a concessão do bónus social de energia elétrica. O fundamento era que a divulgação do código e das informações poderia representar uma potencial violação de direitos de autor, proteção de dados pessoais e segurança da aplicação.

Quando resolvido pelo Supremo Tribunal, este caso poderá estabelecer um precedente para a transparência na utilização de programas e algoritmos por parte das administrações públicas e a potencial limitação do acesso à informação por questões de propriedade intelectual, proteção de dados ou segurança.

Confirmada a sanção ao CSIC por publicar informações incorretamente anonimizadas online

No seu acórdão de 6091/2024, a Audiência Nacional manteve a advertência imposta pela AEPD ao Centro Superior de Investigações Científicas (CSIC) espanhol por ter publicado um documento que revelava a identidade de uma pessoa que exerceu um direito de acesso à informação pública detida pelo referido organismo. Embora no documento existisse um retângulo preto sobre os dados pessoais, o texto não foi removido e pôde ser acedido através de um motor de busca na Internet ou de um editor de PDF, não adotando, por isso, todas as medidas necessárias e violando os artigos 5.º, n.º 1, al. f) e 32.º do RGPD.

Além disso, embora o CSIC alegue que a pessoa que exerceu o direito de acesso à informação pública era uma pessoa que ocupava um cargo público na esfera política e que, portanto, seria do interesse público conhecer a identidade dessa pessoa, a Audiência Nacional confirma que a informação solicitada não estava ligada ao estatuto de titular de cargo público dessa pessoa e pertencia a uma esfera privada de atividade.

Os Estados-Membros podem estabelecer regras mais específicas para garantir a protecção dos direitos e liberdades, mas sem contornar as obrigações de outras disposições do RGPD

O processo C-65/23 decorre de um pedido de decisão prejudicial do Bundesarbeitsgericht (Tribunal do Trabalho Alemão) por resolução de 22 de setembro de 2022, recebido no Tribunal de Justiça em 8 de fevereiro de 2023.

O caso surgiu na sequência de uma denúncia apresentada por um trabalhador da empresa e, ao mesmo tempo, pelo presidente do conselho de empresa, sobre a transferência de dados pessoais de funcionários dessa empresa de um programa informático para um servidor pertencente à empresa-mãe do grupo, localizado nos Estados Unidos. Esta transferência fez parte da implementação de um novo sistema de gestão de pessoal, indo além do que tinha sido acordado em várias resoluções do conselho. Neste contexto, o trabalhador intentou uma ação judicial junto dos tribunais territorialmente competentes na Alemanha (o Arbeitsgericht ou Tribunal do Trabalho, com posterior recurso para o Landesarbeitsgericht ou Tribunal Regional do Trabalho) solicitando o acesso a determinada informação, a eliminação dos dados relativos ao mesmo e a atribuição de uma indemnização.

Não tendo ainda obtido satisfação quanto a este último ponto, o titular recorreu para o Supremo Tribunal do Trabalho (Bundesarbeitsgericht), que é o órgão remetente de diversas questões prejudiciais perante o TJUE. As considerações do Tribunal após a análise das diversas questões concluem que, mesmo que os Estados-Membros se baseiem no artigo 88.º do RGPD para introduzir "regras mais específicas" nos respetivos ordenamentos jurídicos nacionais através de disposições legislativas ou de convenções coletivas, os requisitos decorrentes das restantes disposições do RGPD também devem ser cumpridos. Deste modo, a empresa deveria ter considerado os requisitos do RGPD para o tratamento de dados, incluindo o critério de necessidade discutido no caso concreto. O TJUE estabelece, assim, que, numa convenção coletiva, o artigo 88.º do RGPD não confere às partes um "cheque em branco" para legitimar o tratamento de dados pessoais. Por conseguinte, poderão estabelecer regras nacionais específicas para a proteção de dados no local de trabalho, mas sem fugir às obrigações estabelecidas noutras disposições do RGPD.

Além disso, no seu acórdão de 19 de dezembro de 2024, o TJUE concluiu que, numa convenção coletiva aprovada ao abrigo desse artigo, a margem de apreciação de que as partes dispõem para determinar a necessidade de tratamento não impede o tribunal nacional de exercer um controlo judicial completo.

A recolha de dados sobre os termos de cortesia "senhor" ou "senhora" não pode ser abrangida pela base jurídica da execução de um contrato

No seu acórdão de 9 de janeiro de 2025, C-394/23, o Tribunal de Justiça da União Europeia estabeleceu que a recolha de dados sobre o termo de cortesia (como "senhor" ou "senhora") durante a compra de bilhetes de comboio não é compatível com o Regulamento Geral de Proteção de Dados quando o seu único objetivo é personalizar as comunicações comerciais.

A empresa ferroviária francesa SNCF Connect exigia que os seus clientes utilizassem um termo de cortesia para se dirigir a eles (por exemplo, "senhor" ou "senhora") quando compravam bilhetes online. Este facto foi contestado perante a autoridade francesa de protecção de dados por se ter considerado que essa obrigação é contrária ao RGPD, concretamente ao princípio da minimização de dados, uma vez que não parece ser necessária para executar o contrato de compra de um bilhete de comboio.

O Tribunal de Justiça recorda que, para que o tratamento de dados pessoais seja considerado necessário à execução de um contrato, deve ser objetivamente indispensável para permitir a correta execução desse contrato. Neste caso, o TJUE concluiu que o tratamento de dados com base em termos de cortesia ligados à identidade de género não é objetivamente indispensável à execução de um contrato de transporte. O TJUE considera, assim, que a prática da SNCF Connect é desproporcional e não justifica a recolha de dados pessoais relativos ao termo de cortesia, uma vez que existem alternativas menos invasivas e em conformidade com o RGPD.

O TJUE limita o indeferimento de reclamações por excesso em pedidos de acesso a dados

O caso (processo C-416/23) tem origem numa reclamação apresentada à agência austríaca de proteção de dados Datenschutzbehörde (DSB) por uma pessoa que se queixou de que uma empresa que atua como responsável pelo tratamento de dados não respondeu ao seu pedido de acesso aos seus dados pessoais em tempo útil. No entanto, a DSB recusou-se a atuar em relação a esta queixa devido à sua natureza excessiva, uma vez que o titular dos dados tinha apresentado várias reclamações semelhantes contra diferentes responsáveis pelo tratamento de dados ao longo de um período de aproximadamente vinte meses.

Note-se que, quando uma autoridade de controlo se depara com pedidos manifestamente infundados ou excessivos (entendendo-se como excessivos, na visão do CEPD, os casos de abuso nos termos do artigo 15.º do RGPD, em que os titulares dos dados fazem uso excessivo do direito de acesso com a única intenção de causar danos ou prejuízos ao responsável pelo tratamento), tem a opção de definir uma taxa razoável ou recusar-se a atuar. Contudo, no seu acórdão o TJUE indica que permitir que as autoridades de controlo determinem a natureza excessiva das reclamações apenas porque são em número elevado pode comprometer um nível adequado de proteção de dados pessoais. Embora a multiplicação dos pedidos apresentados por um particular possa constituir um indício da existência de pedidos excessivos quando se verifique que os referidos pedidos não são objetivamente justificados por considerações relativas à proteção dos direitos que lhe são conferidos pelo RGPD, o número dos seus pedidos não pode, por si só, justificar o exercício do poder previsto no artigo 57.º, n.º 4 do RGPD.

4. Atualidade

Foi aprovada uma nova lista de publicidade indesejada validada pela AEPD: Lista Stop Publicidade

No dia 31 de janeiro a AEPD publicou no seu sítio eletrónico um novo ficheiro de exclusão de publicidade designado **Lista Stop Publicidade** ou LSP. Esta é uma alternativa à conhecida Lista Robinson, lançada em 2009 e que, durante mais de quinze anos, foi a única plataforma de exclusão de publicidade em Espanha. O objetivo de ambas é permitir que quem não deseje receber comunicações comerciais limite o seu envio. Para tal, o titular (pessoa singular) apenas necessita de registar os seus dados gratuitamente através do site de um destes sistemas, podendo modificá-los ou cancelar a sua subscrição a qualquer momento. No entanto, é importante referir que, uma vez concluído o registo, as restrições só entrarão em vigor até passados 30 dias.

As diferenças fundamentais entre as duas listas são que a LSP (i) oferece a possibilidade de registar pessoas falecidas e (ii) bloqueia não só chamadas telefónicas, e-mails e mensagens SMS, mas também contas e perfis em redes sociais e aplicações de mensagens.

Por detrás desta iniciativa de criação da LSP está a Associação Espanhola para a Privacidade Digital (Associação EPD), que, como consta na **decisão** da AEPD, apresentou anteriormente três pedidos que foram indeferidos.

A Autoridade Italiana de Proteção de Dados (GARANTE) ordena o bloqueio do DeepSeek em Itália

A Autoridade italiana de Proteção de Dados (*Garante per la protezione dei dati personali*) ordenou com efeitos imediatos a limitação do tratamento de dados dos utilizadores italianos das empresas chinesas que prestam o serviço de *chatbot* do Deep Seek, como já tinha feito com o ChatGPT. Ao mesmo tempo, foi iniciada uma investigação. Esta medida decorre da resposta do Garante ao pedido de informação dos gestores do sistema Hangzhou DeepSeek Artificial Intelligence e Beijing DeepSeek Artificial Intelligence, cujo conteúdo foi considerado completamente insatisfatório.

Neste pedido, o Garante solicitou que as seguintes questões fossem especificadas no prazo de 20 dias: (i) que dados pessoais são recolhidos, (ii) de que fontes, (iii) para que fins, (iv) qual a base legal para o seu tratamento, (v) se os dados são armazenados na China e (vi) se os seus dados provêm de web scraping. Por sua vez, os operadores chineses declararam que não operam em Itália e, por conseguinte, as regulamentações europeias não lhes podem ser aplicadas.
Na mesma linha do Garante, outras autoridades europeias de proteção de dados,

como as da Irlanda e da França, começaram a investigar e a solicitar informações desta inteligência artificial chinesa.

A Comissão Europeia publica orientações sobre práticas proibidas pelo Regulamento de Inteligência Artificial

A Comissão Europeia publicou orientações que detalham e fornecem exemplos práticos para cada uma das práticas de IA proibidas pelo artigo 5.º do Regulamento de IA (por exemplo, sistemas de IA que exibem texto ou imagens demasiado depressa para a mente consciente registar, mas que sejam capazes de influenciar atitudes e comportamentos; sistemas de IA que emitem sons ou imagens de fundo que alteram o estado de espírito do destinatário; etc.).

Relativamente aos sistemas de IA para prever crimes, embora os principais implementadores sejam as agências de segurança pública, as orientações determinam que as atividades de entidades privadas também podem ser abrangidas, por exemplo, nos casos em que as agências de segurança pública confiam a entidades privadas tarefas de prevenção, investigação e acusação de crimes.

Embora não sejam vinculativas, estas orientações procuram garantir a aplicação consistente, eficaz e uniforme do Regulamento de Inteligência Artificial nos vários Estados-Membros da União Europeia, servindo de guia para as autoridades competentes, fornecedores e desenvolvedores de sistemas de IA.

A Autoridade Catalã de Proteção de Dados (APDCAT) apresenta um modelo pioneiro na Europa para o desenvolvimento de soluções de IA que respeitam os direitos fundamentais

A APDCAT apresentou a primeira metodologia da Europa para avaliar o impacto nos direitos fundamentais no domínio da IA aplicada a quatro casos específicos. Esta metodologia foi desenvolvida no âmbito do grupo de trabalho da rede de encarregados de proteção de dados de entidades públicas e privadas da Catalunha (DPD em xarxa).

Os casos previstos pertencem a áreas de atuação onde as soluções de IA são cada vez mais utilizadas: (i) educação (avaliação dos resultados da aprendizagem e previsão do abandono escolar), (ii) gestão de pessoal (sistemas de apoio à decisão na gestão de recursos humanos), (iii) acesso aos cuidados de saúde (tratamento do cancro baseado em imagens médicas) e (iv) serviços de assistência social (assistente de voz para idosos).

Esta metodologia é desenvolvida em três fases: (i) planeamento (descrição do sistema de IA e contexto de utilização), (ii) análise de risco (estimativa do nível de impacto nos direitos) e (iii) mitigação e gestão de riscos.

Chile adota nova Lei de Dados Pessoais

A Lei n.º 21.719, publicada no Diário Oficial a 13 de dezembro de 2024, estabelece um quadro regulatório atualizado para a proteção e tratamento de dados pessoais no Chile. Esta lei modifica as normas de segurança de dados da Lei 19.628 relativa à Proteção da Privacidade e introduz novas bases legais para o tratamento de dados, simplificando e organizando de forma mais eficaz a regulamentação nesta área.

Entre as principais alterações estão novas disposições sobre os direitos dos titulares dos dados, as obrigações dos responsáveis pelo tratamento dos dados, a inclusão de novas categorias de dados, as transferências internacionais de dados e um regime de sanções atualizado.

Além disso, é criada a Agência de Proteção de Dados Pessoais como entidade de controlo, cuja finalidade será assegurar o cumprimento dos direitos relacionados com a privacidade e a proteção de dados pessoais, bem como fiscalizar a lei e exercer outras competências essenciais nesta matéria.

Esta nova regulamentação apresenta desafios significativos, especialmente na esfera tecnológica e ao nível das empresas. Terão de adotar e familiarizar-se com novos padrões de proteção dos dados pessoais que gerem para cumprir eficazmente os regulamentos.

A lei entrará em vigor a 1 de dezembro de 2026.

O Real Decreto 1154/2024, de 19 de novembro, regula a emissão do passaporte provisório e do salvo-conduto

Este decreto estabelece as condições e procedimentos para a obtenção destes documentos, destinados aos cidadãos espanhóis que se encontrem no estrangeiro e não possam obter um passaporte regular num prazo razoável.

Em relação à proteção de dados pessoais, o artigo 17.º do decreto prevê que a emissão de passaportes provisórios e salvo-condutos será regulada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, assim como pela Lei Orgânica 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e de Garantia dos Direitos Digitais.

Mais concretamente, determina-se que os dados pessoais tratados para efeitos do presente decreto real, incluindo a imagem facial ou fotografia do requerente, serão utilizados exclusivamente para verificar a sua identidade e facilitar a sua viagem. O decreto estabelece ainda que as autoridades espanholas garantirão a segurança adequada dos dados pessoais e que estes serão conservados apenas durante o tempo necessário.

No caso de assistência prestada a nacionais de outros Estados-Membros da União Europeia ou aos seus familiares, os dados pessoais não serão conservados por mais de 180 dias após a recolha; e, para os espanhóis que tenham solicitado assistência de representantes de outros Estados-Membros, não mais de dois anos.

Após o termo do período de conservação, os dados pessoais serão eliminados e os documentos devolvidos serão destruídos em segurança.

A AEPD apoia a retenção de dados nos registos de hotelaria, mas sugere que se garanta que são fornecidas cópias aos hóspedes

A AEPD emitiu o Relatório do Gabinete Jurídico 2020-0099 (4 de dezembro de 2024) que analisa o projeto de portaria que altera a Portaria IN/1922/2003, de 3 de julho, sobre livros de registo e formulários de entrada de viajantes em estabelecimentos de hotelaria e similares.

A este respeito, a AEPD recorda o seu Relatório 103/2018 sobre o projeto de decreto real que estabelece as obrigações de registo de documentos e de prestação de informações das pessoas singulares ou coletivas que exercem atividades de alojamento e aluguer de veículos automóveis, destacando que a base jurídica para este tipo de tratamento de dados é o artigo 6.º, n.º 1, alínea c), do RGPD, uma vez que responde a uma obrigação legal imposta aos seus destinatários. No entanto, a AEPD sublinha que a regulamentação de que deriva esta obrigação legal (artigo 25.º, n.º 1 da Lei Orgânica 4/2015, de 30 de março) não contém disposições específicas para adaptar a aplicação do RGPD a este tratamento. Deste modo, de acordo com a AEPD, seria aplicável o critério de que o próprio RGPD contém as garantias mínimas, comuns ou gerais para o tratamento desses dados, desde que o tratamento se refira a dados pessoais que não pertençam a categorias especiais de dados.

Por outro lado, embora a AEPD concorde com o prazo de conservação dos livros de registo de três anos estabelecido no projeto de portaria, adverte que nem a modificação efetuada pelo referido projeto nem a

regulamentação existente na Portaria INT/1922/2003 prevêem que o titular cujos dados são recolhidos e tratados possa obter cópia do documento cuja assinatura é exigida. Consequentemente, sugere-se que o projeto indique claramente que estas folhas do livro de registo serão duplicadas para que o interessado possa obter - se o considerar adequado - um duplicado do que assinar, onde constarão as informações para efeitos da regulamentação sobre proteção de dados; ou prever que o interessado possa obter uma cópia (fotocópia ou similar) do documento assinado em papel ou uma cópia do documento assinado digitalmente.

Para além do acima referido, a AEPD realça que o hoteleiro (enquanto responsável pelo tratamento) deve fornecer ao hóspede/titular todas as informações referidas nos números 1 e 2 do artigo 13.º do RGPD no momento em que o hóspede lê e assina o modelo de documento de entrada de viajantes anexo ao pedido, pois é quando são recolhidos os dados do titular. Refere também, de forma breve, a possibilidade de fornecer essas informações por camadas, de acordo com as disposições do artigo 11.º da LOPDgdd.

Por fim, chama a atenção para o papel das Forças e Órgãos de Segurança do Estado em relação aos dados obtidos através destes formulários, salientando que o mesmo deveria ser definido de forma mais específica, estabelecendo claramente os objetivos e a finalidade deste tratamento.

O CEPD clarifica as regras para a troca de dados com as autoridades de países terceiros e aprova a certificação do selo de proteção de dados da UE

Durante a sua última sessão plenária, que decorreu nos dias 2 e 3 de dezembro de 2024, o Comité Europeu de Proteção de Dados (CEPD) publicou as Orientações sobre o artigo 48.º do RGPD relativas à transferência de dados para autoridades de países terceiros e aprovou um novo selo europeu de proteção de dados.

As orientações acima referidas, que estiveram abertas a consulta pública até 27 de janeiro de 2025, centram-se nos pedidos de cooperação direta entre uma autoridade pública de um país terceiro e uma entidade privada na UE, ao contrário de outras situações em que os dados pessoais são trocados diretamente entre as autoridades públicas da UE e países terceiros. Esses pedidos podem vir de todos os tipos de autoridades públicas, incluindo as autoridades de supervisão do setor privado (por exemplo, do âmbito bancário, fiscal ou segurador), assim como as que estão envolvidas na aplicação da lei e na segurança nacional.

Quanto ao âmbito destas orientações, limita-se a pedidos dirigidos a responsáveis pelo tratamento ou subcontratantes sujeitos ao âmbito territorial estabelecido pelo artigo 3.º, n.º 1 do RGPD. Por outro lado, embora o artigo 48.º não faça qualquer distinção a este respeito, as orientações centram-se nos pedidos feitos diretamente a entidades privadas, uma vez que este é o cenário mais comum, já que os pedidos às autoridades públicas são geralmente enquadrados num quadro de cooperação internacional estabelecido em acordos internacionais.

Por último, o CEPD sublinha que, para além dos requisitos do RGPD, a cooperação com as autoridades públicas de países terceiros pode-se reger por regras adicionais. No entanto, as orientações não entram em detalhes sobre quais podem ser estes requisitos adicionais.

Em relação à aprovação do selo de proteção de dados da UE, o CEPD adotou um parecer que aprova os critérios de certificação de *brand compliance* relativos às atividades de tratamento por parte dos responsáveis ou dos subcontratantes para o tratamento. De referir que, em setembro de 2023, o CEPD já adotou um parecer sobre a aprovação dos critérios nacionais de certificação de *brand compliance* para os Países Baixos. No entanto, os critérios estabelecidos pelo novo parecer serão aplicáveis em toda a Europa e servirão como selo europeu de proteção de dados.

Esta certificação permitirá seguramente às organizações demonstrar a sua conformidade com as normas de proteção de dados, contribuindo para a transparência e confiança dos titulares de dados.

O CEPD apresenta uma carta à Comissão Europeia sobre a revisão das suas onze decisões de adequação adotadas ao abrigo da Diretiva 95/46/CE (6 de dezembro de 2024)

No seu relatório de 15 de janeiro de 2024, a Comissão Europeia concluiu que os dados pessoais transferidos da União Europeia para Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Ilha de Man, Israel, Jersey, Nova Zelândia, Suíça e Uruguai podem continuar a ser transferidos ao abrigo das onze decisões de adequação existentes, adotadas com base no artigo 25.º, n.º 6 da Diretiva 95/46/CE e que se mantinham em vigor nos termos do artigo 45.º, n.º 9 do RGPD.

Em consonância com o acima referido, o Comité Europeu para a Proteção de Dados (CEPD), sem questionar o conteúdo do relatório, apresenta as suas observações à Comissão Europeia numa carta sobre a metodologia a seguir na avaliação de adequação e aponta certos aspetos que poderiam ter sido descritos mais detalhadamente no relatório do CEPD.

O EDPS adverte a Comissão Europeia pela utilização de anúncios direcionados na plataforma X

O EDPS (SupervisorEuropeu de Proteção de Dados) advertiu a Comissão Europeia, na sequência de uma denúncia apresentada pelo grupo NOYB - European Center for Digital Rights ("*None of your business*"), pela utilização de anúncios segmentados na plataforma X durante uma campanha implementada em setembro de 2023 com o objetivo de informar sobre uma proposta de regulamentação para combater o abuso sexual de crianças. Os anúncios foram exibidos 600.000 vezes para perfis de determinadas ideologias políticas e religiões.

A Comissão justificou as suas ações com base no interesse público, com base no RGPD e no Tratado da UE, que estipulam que a Comissão Europeia deve promover o interesse público. No entanto, o EDPS alegou que os cidadãos não poderiam ter previsto este tratamento de dados e que estavam a ser tratadas categorias especiais de dados extraídos de contas privadas, sem ter em conta as exceções previstas no artigo 9.º do RGPD, como a concessão de consentimento pelo titular dos dados ou a existência de dados pessoais que o titular dos dados tenha manifestamente tornado públicos.

O CEPD adotou um parecer sobre a utilização de dados pessoais para o desenvolvimento e implementação de modelos de IA

Este parecer examina 1) quando e como os modelos de IA podem ser considerados anonimizados, 2) se e como o interesse legítimo pode ser utilizado como base jurídica para desenvolver ou utilizar modelos de IA e, em caso afirmativo, como, e 3) o que acontece se um modelo de IA for desenvolvido utilizando dados pessoais que foram tratados ilegalmente. Analisa também o uso de dados próprios e de terceiros.

O parecer foi solicitado pela Autoridade de Proteção de Dados da irlanda (DPA) com o objetivo de procurar a harmonização regulamentar a nível europeu. No seu parecer, o CEPD oferece exemplos de um agente de conversação para auxiliar os utilizadores e o uso de IA para melhorar a cibersegurança.

O parecer inclui também uma série de critérios para ajudar as APD a avaliar se as pessoas podem razoavelmente esperar determinadas utilizações dos seus dados pessoais, incluindo se os dados pessoais estavam disponíveis publicamente, a natureza da relação entre a pessoa e o responsável pelo tratamento, a natureza do serviço, o contexto em que os dados pessoais foram recolhidos,

a fonte a partir da qual foram recolhidos e as possíveis utilizações posteriores do modelo. Examina também o que acontece quando um modelo de IA é desenvolvido utilizando dados pessoais tratadosilegalmente e se isso pode afetar a legalidade da sua implementação.

Noyb denuncia TikTok, Shein e Xiaomi por transferirem ilegalmente dados europeus para a China

A organização NOYB, conhecida por enfrentar gigantes da tecnologia, denunciou as empresas TikTok, Shein, Xiaomi, AliExpress, Temu e WeChat por transferirem dados pessoais de utilizadores europeus para a China, violando o Regulamento Geral de Proteção de Dados (RGPD). As denúncias, apresentadas em cinco países europeus, procuram a suspensão destas práticas e exigem penalizações que podem chegar aos 4% do volume de negócios global das empresas referidas.

Esta é a primeira vez que a NOYB tem como alvo empresas chinesas, acusando-as de enviar dados para um país sem um nível de proteção adequado, conforme exigido pela regulamentação europeia. De acordo com a NOYB, a TikTok, a Shein e a Xiaomi reconheceram estas transferências, enquanto a Temu e a WeChat reconheceram estas transferências para países terceiros para além da China. A organização defende que isto representa uma grave violação dos direitos dos utilizadores europeus.

As empresas defenderam as suas práticas com base no cumprimento regulamentar. O TikTok destacou o seu projeto Clover para o armazenamento de dados na Europa, enquanto a Xiaomi afirmou o seu compromisso com a privacidade e a cooperação com as autoridades. No entanto, as denúncias sublinham a crescente pressão da Europa e de outros países ocidentais contra as empresas tecnológicas chinesas por razões de privacidade, segurança e concorrência desleal.

Uma ação europeia analisa a atenção ao exercício do direito de acesso por parte dos responsáveis

A 20 de janeiro, o Conselho Europeu de Proteção de Dados (CEPD) adotou um relatório sobre a aplicação do direito de acesso pelos responsáveis pelo tratamento de dados. O relatório resume os resultados de uma série de ações nacionais coordenadas realizadas em 2024 no âmbito do Coordinated Compliance Framework (CCF), com a realização de um inquérito em que participou um total de 1185 entidades dos setores público e privado em todo o Espaço Económico Europeu.

O documento enumera os problemas observados por alguns responsáveis, além de uma série de recomendações para os ajudar a implementar o direito de acesso. Um elemento central da análise é o conhecimento dos responsáveis pelo tratamento das Orientações 01/2022 do CEPD sobre os direitos dos titulares de dados - Direito de acesso e se essas orientações foram seguidas na prática.

Os resultados sugerem que é necessária uma maior sensibilização para as Orientações 01/2022, tanto a nível nacional como da UE, uma vez que as orientações ajudam os responsáveis pelo tratamento a implementar o direito de acesso, explicam como o exercício deste direito pode ser facilitado e enumeram exceções e limitações ao mesmo.

Como resultado da ação coordenada em 2024, foram identificados sete desafios. Um deles é resolver a falta de procedimentos internos documentados para processar os pedidos de acesso. Além disso, também foram observadas interpretações inconsistentes e excessivas dos limites do direito de acesso, como o recurso excessivo a certas exceções para negar automaticamente os pedidos de acesso. Para cada desafio identificado, o relatório oferece uma lista de recomendações não vinculativas que os responsáveispelo tratamento de dados e as autoridades de controlo devem considerar.

A AEPD também fez eco desta notícia, na medida em que participou nesta iniciativa coordenada realizada no âmbito do CEPD. A ação coordenada que será realizada ao longo de 2025 centrar-se-á na implementação do direito ao apagamento.

O CEPD publica o Parecer 01/2025 sobre o projeto de decisão da Autoridade de Supervisão Francesa relativa às normas corporativas vinculativas para os responsáveis pelo tratamento de dados do Grupo Coface

Neste parecer, o CEPD conclui que podem ser adotadas regras corporativas vinculativas na medida em que contenham salvaguardas adequadas para garantir que o nível de proteção de pessoas singulares garantido pelo RGPD não é prejudicado quando os dados pessoais são transferidos e tratados pelas organizações do grupo sediadas em países terceiros.

Em qualquer caso, o CEPD recorda que a aprovação de regras corporativas vinculativas não implica a aprovação das transferências específicas de dados pessoais que serão feitas com base nas mesmas. Consequentemente, esta aprovação não pode ser interpretada como uma aprovação de transferências para países terceiros para os quais não seja possível garantir um nível de proteção essencialmente equivalente ao garantido na UE.

A Agência Nacional de Cibersegurança inicia as suas operações e Daniel Álvarez Valenzuela é nomeado diretor

A Agência Nacional de Segurança Cibernética do Chile iniciou oficialmente as suas operações a 1 de janeiro de 2025. O seu principal objetivo é reforçar a segurança digital no país. O seu funcionamento foi formalizado através da publicação no Diário Oficial, em 24 de dezembro de 2024, do Decreto com Força de Lei (DFL) N.º 1-21.663, que regulamenta tanto a sua estrutura organizacional como o seu quadro de pessoal de gestão.

O processo de criação da agência foi liderado pelo Ministério do Interior, e o seu primeiro diretor será Daniel Álvarez Valenzuela, que terá um papel fundamental na gestão da cibersegurança no Chile. Esta nomeação surge no contexto de crescente preocupação com os riscos cibernéticos e da necessidade urgente de uma infraestrutura robusta para proteger a informação crítica das instituições públicas e privadas do país.

A criação da Agência Nacional de Cibersegurança é um passo crucial para reforçar a proteção digital no Chile. A sua implementação, apoiada num quadro regulamentar adequado, permitirá melhorar a capacidade de resposta às ciberameaças, garantindo a segurança das infraestruturas críticas e a integridade da informação.

México: A nova Lei Federal de Proteção de Dados Pessoais na Posse dos Particulares introduz conceitos como o aviso de privacidade e elimina o INAI

No passado dia 21 de março entrou em vigor a nova Lei Federal de Proteção de Dados Pessoais na Posse dos Particulares, que introduz novos conceitos como o aviso de privacidade, consentimento e dados pessoais sensíveis, além de regular o tratamento e a transferência de dados. Também são definidas medidas de autorregulação e estabelecidas sanções por incumprimento.

A publicação completa pode ser consultada neste link.

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

Miguel Ángel Rocha
Counsel · Cidade do México
miguel.rocha@garrigues.com

Alejandra Badillo
Associada sénior · Cidade do México
alejandra.badillo@sanchezdevanny.com

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

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

Carina Casadesús
Júnior · Barcelona
carina.casadesus@garrigues.com

Rocío Álvarez
Júnior · Sevilla
rocio.alvarez@garrigues.com

Juan Luis Serrrano
Sócio · Cidade do México
jlserrano@sanchezdevanny.com

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

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

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

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

Iciar Velasco
Júnior · Madrid
iciar.velasco@garrigues.com

Oriol García
Trainee · Barcelona
oriol.garcia@garrigues.com

Mais informações:

Economia de Dados, Privacidade e Cibersegurança

GARRIGUES

Hermosilla, 3
28001 Madrid
T +34 91 514 52 00
info@garrigues.com

Siga-nos em: