GARRIGUES

Newsletter Economia de Dados, Privacidade e Cibersegurança

Dezembro 2024

Índice

1. Os ‘data centers’ como elemento essencial na economia digital. Desafios e novos horizontes

Um centro de dados (*data center)* é a localização física onde se armazena informação e permite que existam e se desenvolvam os serviços na nuvem (*cloud services)*. Embora esta descrição pareça simples, não o é em absoluto, se tivermos em conta que “a nuvem” é atualmente a própria economia.

Alejandro Padín Vidal

Analisamos a seguir a importância destes *data centers* numa dupla perspetiva: em primeiro lugar, como elemento fundamental na infraestrutura tecnológica dos prestadores de serviços *cloud*; e, em segundo lugar, como potencial elemento crítico do desenvolvimento dos serviços de garantia jurídica baseada em certificação digital, incluindo a identificação eletrónica.

Serviços ‘cloud’ na economia da informação e dos dados

Já ninguém pode ignorar que ativo mais valioso na economia atual (abandonamos o qualificativo de “digital” porque a economia em que vivemos só é, ou é fundamentalmente, digital) é a **informação**. As empresas consideradas principais ou mais importantes do mundo, segundo qualquer dos critérios de análise que utilizemos (faturação, lucros, número de trabalhadores, capitalização bolsista, etc.) são as que construíram o seu valor com base na gestão da informação e, em muitos casos, informação exclusivamente pessoal. Esta realidade é que motivou a atribuição do nome de “economia da informação” ou **“economia dos dados”** à economia global atual.

Paralelamente a esta, ocorre outra realidade no âmbito operacional: a utilização de ferramentas tecnológicas nas empresas, organizações e agentes económicos transferiu-se, e continua a fazê-lo, do mundo físico (*on premise*) para essa nova forma de utilização que são os serviços na nuvem ou serviços *cloud*.

Temos, por isso, duas realidades incontornáveis: a existência de um **ativo com grande valor** como são os **dados** e o **surgimento imparável dos serviços *cloud*** como tendência maioritária na escolha de soluções tecnológicas pelos operadores económicos.

Definidas estas bases, veremos, a seguir, que relação existe entre dados como ativo de valor, os serviços *cloud* e um *data center.*

'Data centers' como peça fundamental de serviços 'cloud'

A atribuição do nome de serviços *cloud* foi uma das opções mais acertadas do marketing setorial da história. Se alguém tem à disposição serviços "na nuvem", tudo parece perfeito. Dá a sensação de que o cliente de serviços tecnológicos na nuvem não tem de se preocupar com nada, porque continua a poder usufruir de todo o serviço tecnológico (seja *software*, plataforma, infraestrutura, etc.) e, além disso, todos os problemas desaparecem: não é necessário espaço nem energia, não são necessários técnicos de manutenção, os equipamentos não se sujam, não faz falta refrigeração nem consumo de eletricidade, o sistema não bloqueia, tudo parece limpo, assético, etéreo, leve… Além disso, a informação já não ocupa espaço nos nossos sistemas, "evapora-se" como por magia e temo-la disponível de forma permanente e contínua, segura e sem riscos. E na verdade, com algumas nuances, tudo isso é uma realidade, mas não porque o serviço *cloud* seja um serviço etéreo prestado a partir da troposfera. Bem pelo contrário, o serviço *cloud* é um serviço prestado com recurso a uma ligação através de redes de telecomunicações entre os nossos equipamentos e a infraestrutura tecnológica do fornecedor. É nessa infraestrutura remota que se armazenam os sistemas e a informação do nosso negócio, sendo precisamente essa a infraestrutura que o prestador dos serviços *cloud* constrói para ser usada na prestação desses serviços. Tudo isso permite à empresa utilizar recursos tecnológicos "como serviço" e mediante pedido, o que lhe confere maior flexibilidade e lhe permite canalizar os custos pela utilização como despesas (OpEx) em vez de como investimentos (CapEx).

Se não fosse aquela opção acertada de marketing, o serviço atualmente conhecido como "na nuvem" poderia perfeitamente designar-se serviço no sótão, pois trata-se de alojar a infraestrutura tecnológica que nos proporciona o serviço, assim como toda a informação que se armazena e processa nesse serviço, num sótão ou num edifício pertencente a um terceiro. Mas esse nome não seria tão atrativo.

Verificamos, por isso, que o *data cente*r é um elemento chave na prestação de serviços na nuvem e que, à medida que a popularidade destes serviços cresce, graças às suas vantagens, as necessidades de espaço e equipamento são também cada vez maiores. Independentemente do tipo de serviços *cloud* que forem prestados (nuvem pública, híbrida, privada) ou do enfoque do *data center* (*hyperscale* para grandes fornecedores, *colocation* para *middle market*, *Edge* para serviços especializados ou de maior proximidade e latência), estamos perante um setor em ascensão e com cada vez mais oportunidades de se desenvolver ao abrigo da regulação da economia digital.

Perspetiva regulatória e valor como ativo essencial para a economia

A economia dos dados, da informação… enfim, a economia em que vivemos e da qual vivemos é liderada por empresas que, tal como dissemos, geram o seu valor com base na gestão direta ou indireta de informação e dados. Quatro das cinco maiores empresas do mundo, em termos de capitalização bolsista em 2024, são empresas digitais ou tecnológicas, seis das dez primeiras. A grande maioria das cem principais empresas em termos de capitalização, são tecnologicamente dependentes ou utilizam serviços na nuvem de forma intensiva.

Tal como afirmámos, os *data centers* são a infraestrutura onde se armazenam os equipamentos e os sistemas essenciais para a prestação de serviços *cloud*. Atendendo a que "a nuvem" não é uma nuvem mas um sótão ou um edifício, percebemos como esta peça é essencial nos fluxos económicos dos serviços *cloud*.

Por outro lado, os *data centers* terão sempre de se localizar próximo do utilizador, por motivos tanto tecnológicos como regulatórios. Do ponto de vista tecnológico, a evolução de determinadas soluções exige requisitos de latência muito baixa, o que implicará proximidade entre a fonte dos dados e das ferramentas de tratamento e o utilizador. Do ponto de vista regulatório, especialmente

na União Europeia, existem normas que obrigam a manter e a tratar os dados dentro do território da União, com exigências muito rigorosas para poder transferir esses dados para fora do território comunitário. Estas normas tiveram um efeito crescente, pois muitas empresas, especialmente em setores críticos, exigem aos seus prestadores de serviços *cloud* que mantenham os dados armazenados dentro do território da União ou até do próprio país. Se, tal como vimos, o *data center* é o elemento do serviço *cloud* onde se armazenam os dados, para cumprir essas exigências terá de estar localizado, necessariamente, no território do país ou da União.

Daí decorrem, adicionalmente, outras necessidades no âmbito jurídico, pois a localização em determinado território de um *data center*, considerando a sua importância, faz com que incidam sobre estas infraestruturas as normas aplicáveis à segurança da informação (como na UE, a Diretiva NIS 2, o Regulamento DORA e outras diretivas e regulamentos de cibersegurança) ou à privacidade dos dados (RGPD e normas setoriais).

Futuro do 'data center' como elemento da garantia jurídica digital

O que explicamos até aqui já nos permite ver o valor e a importância dos *data centers* na economia, mas há mais. Terminamos com uma ideia de futuro mas não menos aliciante e importante que a anterior.

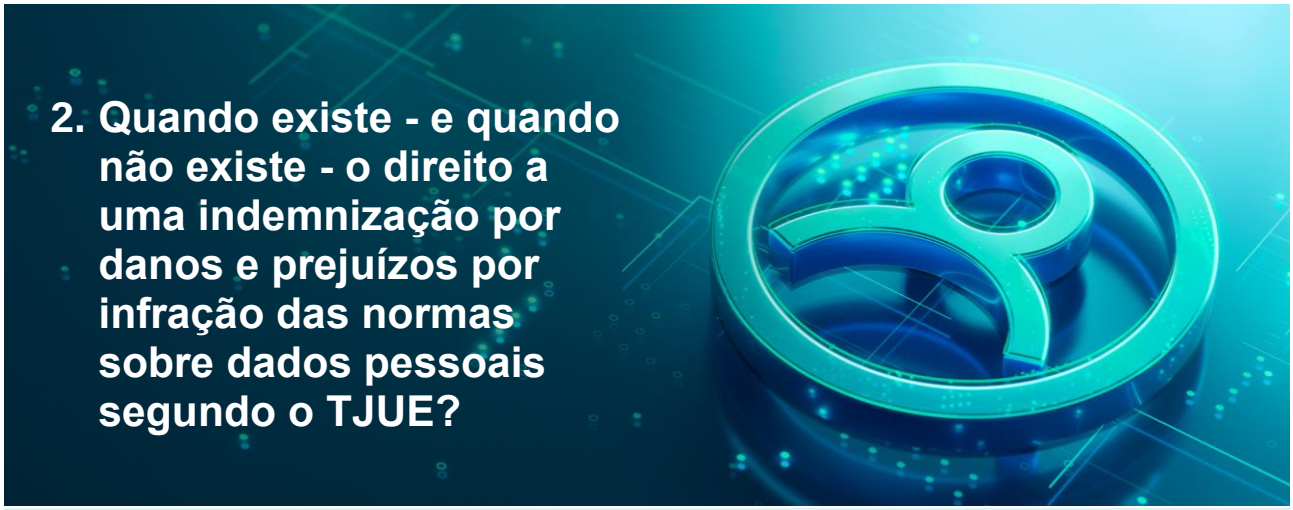
Na evolução da economia digital, da informação ou dos dados, a estação seguinte é a da **segurança digital** e da **identificação digital**. À medida que a economia tradicional se vai transferindo, até acabar por se basear na nuvem, é essencial consolidar definitivamente nesse âmbito a necessária segurança jurídica, equivalente à que existe no mundo físico. Para isso, são fundamentais os serviços de certificação da identidade através de tecnologia baseada em certificação digital, que na União Europeia é regulada pelos regulamentos eIDAS e eIDAS 2.

Esta regulamentação estabelece que a certificação da identidade através da utilização de certificados eletrónicos qualificados ou a certificação de eventos e documentos digitais através da utilização de certificados temporais qualificados, têm o mesmo valor legal que o ato jurídico equivalente realizado no mundo físico. Para usar um exemplo de fácil compreensão, um contrato assinado com assinatura digital qualificada (baseada num certificado eletrónico qualificado) tem pleno valor legal, sendo essa assinatura equivalente à assinatura manuscrita, mas, além disso, com presunção de veracidade em caso de impugnação por terceiros. De igual modo, um documento eletrónico (escrito, gráfico, audiovisual…) em que seja inserido um carimbo temporal qualificado é prova bastante, com pleno valor jurídico, do ato que faz parte integrante desse documento eletrónico, com presunção de veracidade.

Neste contexto, é fundamental decidir onde se integram esses certificados eletrónicos e, acima de tudo, quem os integra, pois é necessária a participação de uma entidade regulada, um terceiro de confiança oficialmente qualificado que emita esses certificados reunindo todas as formalidades e requisitos exigidos pela norma para que esse ato tenha a máxima validade legalmente prevista. Neste sentido, se a emissão dos certificados se junta ao armazenamento da informação ou ao tratamento dessa informação no próprio *data center*, estaremos a converter estes centros num elemento diretamente inerente à confiança digital e aos serviços tecnojurídicos que são o futuro da economia.

Isso implicará a necessária colaboração entre entidades de confiança reguladas, emitentes de certificados eletrónicos qualificados e os promotores ou gestores de *data centers*. Para potenciar esta aliança, deverão ser integrados especialistas em regulação que apoiem a procura de soluções para os problemas de segurança jurídica digital, dando uma dimensão de garantia legal à solução tecnológica conjunta.

Este artigo deverá servir para que o mercado reflita com os olhos postos no futuro e para que as empresas se certifiquem de que possuem a tecnologia e a assessoria jurídica para conseguir chegar a essa próxima estação e promover o próximo troço da rota da evolução tecnológica sobre bases sólidas e solventes



2. Quando existe - e quando não existe - o direito a uma indemnização por danos e prejuízos por infração das normas sobre dados pessoais segundo o TJUE?

A violação das normas em matéria de proteção de dados pode envolver, além das sanções a aplicar pelas autoridades competentes, a obrigação de indemnizar os afetados que tenham sofrido danos e prejuízos. O Tribunal de Justiça da União Europeia (TJUE) pronunciou-se recentemente sobre a matéria, criando um corpo jurisprudencial que configura os requisitos e limites da responsabilidade civil neste âmbito. Nesta publicação analisamos os critérios definidos até ao momento pelo TJUE.

Cecilia Rosende, Ana López**, Alberto Pimenta** y **Antonio Entrena**

O Regulamento 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 (RGPD), estabeleceu o direito de as pessoas que tenham sofrido danos materiais ou imateriais devido a uma infração serem indemnizadas por esses danos (artigo 82.º).

Previu também a possibilidade de tutela coletiva perante este tipo de infrações, de modo que os afetados possam autorizar determinadas entidades, organizações ou associações sem fins lucrativos a apresentar reclamações em seu nome (artigo 80.º).

Neste contexto, surgiram dúvidas sobre os pressupostos do referido direito a uma indemnização, o que deu lugar à apresentação junto do TJUE de diversas questões prejudiciais, até agora em relação a ações individuais.

As questões suscitadas junto do TJUE pelos tribunais nacionais foram muito variadas: desde se a existência de infração das normas sobre dados pessoais dá lugar, em qualquer caso, a um direito à indemnização, até qual é o regime de responsabilidade, passando pelas causas de exoneração, entre outras.

E essas dúvidas colocaram-se em diversas situações, tais como: tratamento não consentido de dados relativos a afinidades políticas (acórdão de 4 de maio de 2023, processo C-300/21, *Österreichische Post AG*); reclamação em caso de ciberataque e publicação dos dados pessoais na Internet como consequência daquele (acórdão de 14 de dezembro de 2023, processo C-340/21 *Natsionalna agentsia za prihodite*); divulgação sem consentimento de dados pessoais num site de uma autarquia local, mais concretamente na ordem do dia de uma sessão do Conselho Municipal em relação a uma acórdão judicial (acórdão também de 14 de dezembro de

2023, processo C-456/22**,** *Gemeinde Ummendorf*); tratamento por um empregador de dados relativos à saúde de um trabalhador (acórdão de 21 de dezembro de 2023, processo C-667/21, *Medizinischer Dienst der Krankenversicherung Nordrhein*); entrega por erro a um terceiro dos documentos de uma compra em que constavam dados pessoais, incluindo bancários e receitas de um cliente (acórdão de 25 de janeiro de 2024, processo C-687/21**,** *MediaMarktSaturn*); receção de comunicações comerciais, apesar de o titular ter declarado expressamente a sua oposição às mesmas (acórdão de 11 de abril de 2024, processo C-741/21**,** *juris GmbH*); divulgação a terceiros, por erro, da declaração tributária dos afetados (acórdão de 20 de junho de 2024, processo C-590/22, *PS*); roubo por terceiros de dados pessoais registados numa aplicação de negociação com valores (acórdão também de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*); difusão de uma sequência de vídeo cujo personagem imitava o requerente, que era um conhecido jornalista, sem que este tivesse dado o seu consentimento (acórdão de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs*); ou publicação de dados pessoais não exigidos legalmente no Registo Comercial de um Estado-Membro (acórdão também de 4 de outubro de 2024, processo C-200/23**,** *Agentsia po vpisvaniyata*).

Embora continuem a ser levantadas questões prejudiciais, podem ser extraídos das decisões do TJUE proferidas até ao momento os critérios indicados a seguir.

Critérios do TJUE

1. Não existe um "direito automático a ser indemnizado" como consequência de uma violação das normas de proteção de dados

A **mera existência de uma violação** das normas de proteção de dados **não gera automaticamente um direito a ser indemnizado**. Para isso, é necessário que concorram, de forma cumulativa, os seguintes **três requisitos**: i) a existência de uma **infração** das disposições do RGPD; ii) que o afetado tenha sofrido **danos e prejuízos**; e iii) uma **relação de causalidade** entre a infração e os danos e prejuízos.

Assim o definiu o TJUE claramente, pela primeira vez, na acórdão de 4 de maio de 2023, processo C-300/21, *Österreichische Post AG* (pp. 32 – 36 e 42) e assim continuou, sem desvios, nas decisões posteriores (acórdãos de 14 de dezembro de 2023, processo C-340/21 *Natsionalna agentsia za prihodite*, p. 77; também de 14 de dezembro de 2023, processo C-456/22, *Gemeinde Ummendorf*, p. 14; de 21 de dezembro de 2023, processo C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, p. 82; de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, p. 58; de 11 de abril de 2024, processo C-741/21, *juris GmbH*, p. 34; de 20 de junho de 2024, processo C-590/22, *PS*, pp. 22 e 24-25; também de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, pp. 41-42 e 57; de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* pp. 24 e 26-27) ou também de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, pp. 140 e 159).

2. Enquanto o conceito de danos e prejuízos indemnizáveis se rege pelo direito da União, o montante dos danos será determinado de acordo com cada direito nacional

Na medida em que não haja uma remissão expressa para o direito dos Estados-Membros, o conceito de "**danos e prejuízos materiais ou imateriais**" e o conceito de "**indemnização pelos danos e prejuízos sofridos**" previsto no artigo 82.º do RGPD terão de ser objeto de **interpretação autónoma**. Ou seja, que a interpretação a fazer se regule pelo direito da União, devendo interpretar-se de modo uniforme em todos os Estados-Membros, não tendo de coincidir com a interpretação que, relativamente aos referidos conceitos, poderia ser feita de acordo com a legislação nacional de cada Estado-Membro (acórdãos 4 de maio de 2023, processo C-300/21, *Österreichische Post*

AG, pp. 29-30 e 44 ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 139).

No entanto, e na medida em que o RGPD não contém qualquer disposição a esse propósito, a **determinação** ou **quantificação da indemnização reger-se-á de acordo com o direito nacional de cada Estado-Membro**, devendo respeitar-se, em qualquer caso, os princípios de equivalência e eficácia (acórdãos de 4 de maio de 2023, processo C-300/21, *Österreichische Post AG*, pp. 54 e 59; de 21 de dezembro de 2023, processo C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, pp. 83 e 101; de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, p. 53; de 11 de abril de 2024, processo C-741/21, *juris GmbH*, pp. 58 e 63; de 20 de junho de 2024, processo C-590/22, *PS*, p. 40; também de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, pp. 27 e 33; de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* p. 32 e também de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 152).

Mais concretamente, como sublinhou a doutrina mais acolhida, em situações transfronteiriças, serão as normas de conflitos de cada Estado-Membro que determinarão a legislação nacional aplicável, pois o Regulamento (CE) n.° 864/2007 relativo à lei aplicável às obrigações extracontratuais (Regulamento Roma II) exclui do seu âmbito de aplicação as obrigações extracontratuais que decorram da violação da vida privada e dos direitos de personalidade (artigo 1.º, n.º 2, alínea g) do Regulamento Roma II). Em Espanha, a norma de conflitos aplicável será o artigo 10.º, n.º 9 do Código Civil (que dispõem que "as obrigações não contratuais serão reguladas pela lei do lugar onde tenha ocorrido o facto de que decorram").

A isto acresce que, segundo o artigo 79.º, n.º 2 do RGPD, serão competentes tanto os tribunais do Estado-Membro em que o responsável ou encarregado tenha um estabelecimento, como os tribunais do Estado-Membro em que o titular tenha a sua residência habitual (salvo se o responsável ou encarregado for uma autoridade pública de um Estado-Membro que atue no exercício dos seus poderes públicos). E esta dualidade de foros (além de se aplicarem eventualmente os previstos no Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de acordo com o Considerando 147 do RGPD) poderia levar a situações de *forum shopping,* de modo a recorrer aos tribunais da jurisdição que possa ser mais favorável.

3. Alcance da indemnização

a. Danos e prejuízos materiais ou imateriais

O titular terá direito a ser indemnizado **tanto pelos danos e prejuízos materiais como pelos danos imateriais sofridos** (como, por exemplo, danos morais), **sem que se exija** que **atinjam um determinado limiar de gravidade** (acórdãos de 4 de maio de 2023, processo C-300/21, *Österreichische Post AG* -pp. 45 – 51-; de 14 de dezembro de 2023, processo C-340/21 *Natsionalna agentsia za prihodite* p. 78; de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, pp. 59 e 60; de 11 de abril de 2024, processo C-741/21, *juris GmbH*, pp. 36 e 41; de 20 de junho de 2024, processo C-590/22, *PS*, p. 26; também de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, p. 44; ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 149).

O próprio RGPD (Considerando 85) destaca que "[s]e não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de

confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares".

Para que o dano seja indemnizável, terá de ser **comprovada** a sua **existência e consequências negativas** (acórdãos de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, pp. 60 e 61; de 20 de junho de 2024, processo C-590/22, *PS*, pp. 34 e 35; ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, pp. 141-142).

O **receio** que **um afetado sente de um potencial uso indevido** por terceiros dos seus dados pessoais no futuro, na sequência de uma infração, **poderia constituir um dano imaterial indemnizável**, embora tenha de se comprovar que esse receio tem **fundamento** (acórdãos de 14 de dezembro de 2023, processo C-340/21 *Natsionalna agentsia za prihodite*, pp. 83-85; de 20 de junho de 2024, processo C-590/22, *PS*, p. 32; ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, pp. 143-144).

Além disso, a **perda de controlo sobre os dados pessoais durante um breve período de tempo** poderá provocar ao titular "danos e prejuízos imateriais" que dêem lugar a um **direito a ser indemnizado**, **se** o titular demonstrar que **sofreu efetivamente esses danos e prejuízos, por mínimos que sejam** (acórdãos de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, p. 66; de 20 de junho de 2024, processo C-590/22, *PS*, p. 33; ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 150).

Como se indicou anteriormente, a mera infração das normas de proteção de dados não confere aos afetados, *per se*, o direito a exigir uma indemnização ao infrator. É necessário que **comprovem** que **sofreram efetivamente os danos e prejuízos reclamados, mesmo quando estes sejam de pouca monta** (acórdão de 14 de dezembro de 2023, processo C-456/22, *Gemeinde Ummendorf*, p. 22). Assim, um **risco meramente hipotético de uso indevido dos dados pessoais por um terceiro não autorizado não pode dar lugar a indemnização** se, por exemplo, se demonstrar que **nenhum terceiro teve conhecimento dos dados pessoais em causa** (acórdão de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, p. 68).

Por fim, o TJUE estabeleceu que, **quando o prejuízo sofrido pelo titular não tenha gravidade, o órgão jurisdicional nacional poderá reconhecer uma indemnização mínima**, sempre que tal montante pouco elevado de indemnização concedido nesses termos possa ressarcir integralmente o prejuízo (acórdãos de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, pp. 45-46 e de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* p. 35). Mesmo a apresentação de um pedido de desculpa poderia constituir uma reparação autónoma ou complementar de um dano moral, conforme previsto no direito nacional aplicável; em particular quando seja impossível restabelecer a situação anterior à ocorrência do dano e sempre que esta forma de reparação possa compensar integralmente o prejuízo sofrido pelo titular (acórdão de 4 de outubro de 2024, processo C-507/23, *Patērētāju thiesību aizsardzības centrs,* pp. 36 y 37).

b. **Função compensatória, não punitiva**

O direito a ser indemnizado, previsto no artigo 82.º do RGPD, tem uma **função compensatória**, de modo que a indemnização pecuniária deve compensar integralmente os danos e prejuízos sofridos como consequência da infração. Assim, **não** se enquadra neste direito impor o pagamento de indemnizações de **carácter punitivo** (acórdão de 4 de maio de 2023, processo C-300/21, *Österreichische Post AG*, pp. 57 e 58; de 21 de dezembro de 2023, processo C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, p. 84 e 102; de 25 de janeiro de 2024, processo C-687/21, *MediaMarktSaturn*, p. 47; de 11 de abril de 2024, processo C-

741/21, *juris GmbH*, pp. 60 e 61; de 20 de junho de 2024, processo C-590/22, *PS*, pp. 41-42; de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* p. 34 ou também de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 153).

Na medida em que a imposição de sanções administrativas, por um lado, e a determinação de indemnizações, por outro, respondem a âmbitos normativos distintos, não se aplicam a estas últimas os critérios daquelas (acórdãos de 11 de abril de 2024, processo C-741/21, *juris GmbH*, p. 57; de 21 de dezembro de 2023, processo C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, pp. 85 e 86, de 20 de junho de 2024, processo C-590/22, *PS*, p. 43; também de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, pp. 22, 39 e 44; ou de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* pp. 39 a 41).

Deste modo, e dada a função exclusivamente compensatória da indemnização, elementos como o nível de gravidade ou o carácter eventualmente doloso da infração por parte do responsável pelo tratamento não serão tidos em conta para efeitos da reparação do dano, mas apenas o prejuízo sofrido pelo titular (acórdãos de 11 de abril de 2024, processo C-741/21, *juris GmbH*, p. 64; de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital*, pp. 28-30; ou de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* pp. 42-43), sem que se possa considerar, em princípio, que as lesões corporais são, pela sua própria natureza, mais importantes do que os danos imateriais (acórdãos de 20 de junho de 2024, C-182/22 y C-189/22, *Scalable Capital*, pp. 38 e 39 ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 151).

Por sua vez, nem a atitude e a motivação do responsável pelo tratamento devem ser tidos em conta para conceder uma indemnização de um "nível inferior" à compensação integral do prejuízo sofrido pelo titular (acórdão de 4 de outubro de 2024, processo C-507/23, *Patērētāju tiesību aizsardzības centrs,* pp. 44-45).

c. **O regime de responsabilidade por culpa com inversão do ónus da prova**

O **afetado** terá de comprovar a **existência da infração e** dos **danos e prejuízos sofridos**, enquanto o **responsável pelo tratamento dos dados pessoais ou o subcontratante** terá de provar a **ausência de culpa no facto** que originou os danos e prejuízos se pretender exonerar-se de responsabilidade, pois presume-se a existência de culpa (acórdãos de 21 de dezembro de 2023, processo C-667/2, *Medizinischer Dienst der Krankenversicherung Nordrhein*, pp- 93-94, 98-99 e 103; de 11 de abril de 2024, processo C-741/21, *juris GmbH*, pp. 46 e 47; de 20 de junho de 2024, C-182/22 e C-189/22, *Scalable Capital* p. 28; ou de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, p. 154 e pp.160-164) ou a **falta de relação de causalidade** entre a eventual infração de proteção de dados e os danos e prejuízos sofridos pelo titular (acórdão de 14 de dezembro de 2023, *Natsionalnaagentsia za prihodite*, C-340/21, pp. 70 e 72).

Deste modo, quando a violação da segurança dos dados pessoais tenha sido praticada por **cibercriminosos**, o **responsável** pelo tratamento pode ficar **exonerado** de responsabilidade, **se demonstrar que não incumpriu as obrigações de proteção de dados** a que está sujeito (acórdão de 14 de dezembro de 2023, *Natsionalnaagentsia za prihodite*, C-340/21, pp. 70-72).

Por sua vez, o responsável pelo tratamento **não se iliba** alegando **negligência ou incumprimento de uma pessoa que atue sob a sua autoridade**, na medida em que lhe cabe certificar-se de que os seus funcionários aplicam corretamente as suas instruções (acórdão de 11 de abril de 2024, processo C-741/21, *juris GmbH*, pp. 49 e 52). Como **também não** exonera

de responsabilidade a **existência de um parecer consultivo e não vinculativo** emitido por uma autoridade de controlo dirigido ao responsável pelo tratamento (acórdão de 4 de outubro de 2024, processo C-200/23, *Agentsia po vpisvaniyata*, pp. 174 - 176).

Conclusão

Não são raros os casos em que os afetados por violações de dados pessoais procuram apurar a responsabilidade civil de quem incorreu na violação correspondente.

Por isso, é fundamental ter em conta a delimitação de responsabilidades que o TJUE tem vindo a fazer, uma vez que a mera existência de uma violação da regulamentação sobre dados pessoais não determina automaticamente que surja uma obrigação de indemnização, mas esta só existirá quando, de forma efetiva e causal, tenham ocorrido danos para os afetados, que terão ser comprovados, por mínimos que sejam. Além disso, as indemnizações devem destinar-se a compensar os danos e prejuízos sofridos, mas não podem, em caso algum, ter um carácter punitivo ou dissuasor.

3. Resoluções das autoridades de proteção de dados

Rede hospitalar sancionada com 200.000 euros por incumprir o artigo 32.º do RGPD, quanto à manutenção de um 'software' de registos clínicos eletrónicos e faturação

A resolução PS-00351-2023 de 30 de setembro de 2024 é proferida na sequência de uma reclamação contra uma rede hospitalar apresentada à AEPD por deficiências de segurança na manutenção do software utilizado em todos os seus centros hospitalares para a gestão de registos clínicos eletrónicos e faturação.

No âmbito do procedimento, a Agência Espanhola de Proteção de Dados (AEPD) iniciou diligências prévias de investigação para analisar o contrato de subcontratação de tratamento entre o hospital e o fornecedor do *software*, as análises de riscos e avaliações de impacto realizadas, assim como as medidas de segurança implementadas.

A AEPD identificou varias deficiências nas medidas de segurança do hospital, incluindo a falta de rastreabilidade de acessos, a ausência de auditorias específicas do *software* e a insuficiência do sistema de encriptação de dados.

Embora o hospital, por sua vez, tenha implementado várias medidas corretivas durante o procedimento - como a melhoria do sistema de encriptação e a limitação do número de utilizadores com autorizações de administração -, a AEPD conclui que este não tinha implementado as medidas de segurança adequadas, como um sistema robusto de encriptação e auditorias regulares, o que constitui uma violação do artigo 32.º do RGPD. Além disso, a AEPD realça que o hospital, ao ter celebrado contratos com o setor público para a prestação de serviços de saúde desde o ano 2022, está obrigado a cumprir o Esquema Nacional de Segurança, não tendo sequer cumprido os requisitos impostos por esse esquema.

Assim, aplica-se ao hospital uma coima de 200.000 euros pela violação do artigo 32.º do RGPD, tipificada no artigo 83.º, n.º 4 do RGPD, tendo em conta a negligência do hospital ao não implementar medidas de segurança adequadas, a ligação da sua atividade ao tratamento de dados pessoais em grande escala (incluindo categorias especiais de dados) e a falta de auditorias específicas ao *software* utilizado.

AEPD impõe uma sanção por violação do artigo 6..º, n.º 1 do RGPD por ceder e incluir os números de telefones particulares de polícias locais num plano de emergência de uma autarquia local

Este procedimento sancionatório foi iniciado por causa de duas reclamações apresentadas

junto da AEPD pelo Sindicato *Unión de Policía Municipal* e um particular, em que se denunciava uma eventual violação em matéria de proteção de dados por parte de uma autarquia local, por ter incluído e cedido de forma não autorizada os números de telemóvel particulares dos funcionários policiais nos Planos de Emergência elaborados por uma empresa consultora.

Durante a realização de simulacros de incêndios em janeiro de 2023 na Unidade Integral de uma determinada Esquadra da Polícia Municipal, foi usado pelo pessoal policial um documento designado "Plano de Emergência" que continha um "Diretório de Comunicação" com os dados pessoais e números de telemóveis particulares dos funcionários policiais. Estes dados não tinham sido fornecidos nem autorizados para este efeito pelos polícias envolvidos, e a Direção-Geral da Polícia Municipal tinha-os disponibilizados à empresa consultora sem o conhecimento nem o consentimento dos afetados. Além disso, verificou-se que noutras unidades policiais eram utilizados números de telefone fixo em vez de telemóveis particulares, e que alguns dos funcionários listados no diretório já estavam reformados, tinham mudado de unidade ou estavam em situação de incapacidade temporária.

Na resolução PS-00374-2023 de 4 de outubro de 2024, a AEPD determinou que o tratamento dos dados pessoais dos polícias, mais especificamente os seus números de telemóveis particulares, não cumpria qualquer das condições de licitude estabelecidas no artigo 6.º, n.º 1 do RGPD. Não foi obtido o consentimento dos titulares, nem se justificou a necessidade do tratamento para o cumprimento de uma obrigação legal, a execução de um contrato, a protecção de interesses vitais, o cumprimento de uma missão de interesse público ou a satisfação de interesses legítimos.

Por sua vez, a autarquia local argumentou que a inclusão dos referidos números era necessária para a coordenação em situações de emergência, nos termos da Lei 17/2015 do Sistema Nacional de Proteção Civil e do Real Decreto 393/2007. No entanto, a AEPD concluiu que nenhuma norma exigia especificamente a utilização de números de telemóveis particulares e que noutros planos de emergência se utilizavam números de telefone fixo.

Tanto a autarquia local como a empresa consultora eliminaram os dados pessoais dos Planos de Emergência apos serem informadas da violação, tendo a AEPD ponderando positivamente esta ação corretiva. A AEPD deliberou que a autarquia local tinha violado o artigo 6.º, n.º 1 do RGPD, tipificado como uma violação muito grave no artigo 83.º, n.º 5, al. a) do RGPD e o artigo 72.º, n.º 1, al. b) da LOPDGDD. A resolução declarou a violação e ordenou a notificação da mesma ao Provedor de Justiça, mas não foram impostas medidas complementares atendendo à eliminação dos dados pessoais já realizada pela autarquia local e pela empresa consultora.

A AEPD impõe uma multa de 50.000 euros por não serem protegidos corretamente os dados dos trabalhadores num processo de mediação por assédio no local de trabalho

A parte reclamante, uma trabalhadora de uma conhecida empresa de saúde e segurança no trabalho, apresentou uma denúncia à Inspeção do Trabalho e Segurança Social por uma possível situação de assédio no local de trabalho. A empresa transmitiu no seu relatório final de mediação para a Inspeção todos os dados pessoais da parte reclamante e também dos denunciados.

Na sua resolução PS-00012024, a AEPD considera que foi violada a integridade e confidencialidade do tratamento prevista nos artigos 5.º, n.º 1, al. f) (princípio da integridade e confidencialidade) e 32.º (segurança do tratamento) do RGPD.

A AEPD conclui que não foi cumprido o dever de diligência exigível, incluindo ainda vários fatores agravantes, como a natureza e o alcance, a intencionalidade ou negligência, a categoria dos dados e a ligação da atividade

do infrator ao tratamento de dados pessoais, e aplica uma coima de 30.000 euros por violação da alínea f) do n.º 1 do artigo 5.º do RGPD e outra coima de 20.000 euros por violação do artigo 32.º do RGPD. Além disso, no entender da AEPD, a empresa não comprovou as medidas de segurança de que dispõe para evitar que os documentos incluam dados pessoais não anonimizados.

A cessão ilegítima de dados pessoais pode implicar uma coima de 100.000 euros

Na sua resolução PS-00245-2024 a AEPD aplica uma sanção a uma empresa de eletricidade ao concluir que determinados dados da pessoa singular reclamante tinham sido cedidos diretamente a uma empresa de eletricidade para a formalização de um contrato de fornecimento de eletricidade, quando o reclamante nunca tinha mantido qualquer comunicação nem relação com essa empresa de eletricidade.

A empresa fornecedora explica na sua resposta à AEPD que, no processo de envio do contrato ao reclamante, ocorreu um erro por parte da pessoa que recebeu o pedido, por força do qual ocorreu uma confusão entre as duas entidades a quem o operador prestava serviços.

Neste caso, a AEPD considera que ficou provado que a reclamada violou o artigo 6.º, n.º 1 do RGPD, uma vez que realizou o tratamento dos dados pessoais da parte reclamante sem legitimidade para tal. Embora a parte reclamada afirme que os factos foram consequência de um erro do comercial, essa circunstância não afasta o facto de ter ocorrido o tratamento indevido, nem supre a falta de legitimidade para realizar esse tratamento, fixando-se a sanção no montante de 100.000 euros por violação do artigo 83.º, n.º 5, al. a) do RGPD.

AEPD impõe uma coima de 300.000 euros a um banco por aceder a dados pessoais contidos num ficheiro de património sem ter qualquer relação contratual com o titular

O reclamante tinha celebrado um empréstimo hipotecário com a entidade bancária, cuja falta de pagamento originou um procedimento judicial de reclamação de dívida, sendo o processo resolvido mediante pagamento extraprocessual com a assinatura de uma transação entre as partes. Após a assinatura, o reclamante teve conhecimento de que a entidade financeira tinha acedido aos seus dados pessoais existentes no ficheiro de património até 47 ocasiões após a data do referido acordo.

Na sua resolução PS-00380-3034 de 22 de outubro, a AEPD sustenta que o artigo 20.º, n.º 1, al. e) da LOPDGDD presume um tratamento lícito dos dados pessoais de um particular quando são consultados na base de dados do ficheiro de solvência patrimonial por quem mantiver uma relação contratual com o afetado que implique o pagamento de um valor, ou este tenha solicitado a celebração de um contrato que implique financiamento, pagamento diferido ou cobrança periódica. No entanto, neste caso a consulta dos dados pessoais do reclamante foi feita depois de terminada a relação contratual, pelo que a entidade bancária não tinha uma base legal para esse acesso.

Conforme o que antecede, a AEPD aplica uma coima de 300.000 euros à entidade bancária por violação do artigo 6.º, n.º 1 do RGPD.

AEPD aplica uma sanção de 30.000 euros por cada site de uma empresa reincidente no incumprimento em matéria de 'cookies'

Na resolução PS-00524-2023, a AEPD decide um processo sancionador contra uma entidade prestadora de serviços da sociedade

da informação e titular de vários sites por incumprimento do artigo 22.º, n.º 2 da Lei 34/2022, relativa aos serviços da sociedade da informação e de comércio eletrónico, no que se refere à utilização de *cookies* e à informação incluída em cada uma das políticas de *cookies*. A AEPD deteta uma série de deficiências, como a utilização de *cookies* tanto próprios como de terceiros, embora o utilizador não tenha aceitado essa utilização, ou a falta de informação sobre *cookies* de terceiros instalados aquando do início da navegação web.

Esta mesma entidade já foi multada anteriormente pela AEPD por, entre outros, incumprimento do art.º 22.º, n.º 2 da LSSI, no valor de 5.000 euros por site. Neste caso, considerando como agravante a reincidência por prática de uma infração da mesma natureza, a AEPD aplica à empresa uma coima de 30.000 euros por cada site (90.000 euros no total).

Autoridade de proteção de dados irlandesa (DPC) aplica uma multa de 310.000.000 euros à LinkedIn por realizar análise comportamental e publicidade personalizada sem base legal

Na sequência de uma reclamação de uma organização francesa sem fins lucrativos, a DPC profere uma resolução sobre o tratamento pela LinkedIn de dados pessoais dos utilizadores desta rede social para efeitos de análise comportamental e publicidade personalizada sem dispor de uma base legal adequada (nota de imprensa). A DPC determina que não se pode basear (i) no consentimento, uma vez que o consentimento obtido não foi livre, suficientemente informado nem específico; (ii) no interesse legítimo, pois os interesses da LinkedIn não prevalecem sobre os dos titulares; nem (iii) na execução do contrato, pois a realização deste tratamento não é necessária para a execução do contrato. A DPC conclui que a LinkedIn violou o artigo 6.º do RGPD, assim como o princípio da licitude, lealdade e transparência previsto no artigo 5..º, n.º 1, alínea a) do RGPD. Além disso, a DPC considera que a entidade não cumpriu o dever de informar devidamente os utilizadores (artigos 13.º e 14.º do RGPD).

Pelos incumprimentos anteriores, a DPC aplica à LinkedIn coimas que atingem um total de 310.000.000 euros.

Autoridade de proteção de dados italiana (Garante) impõe uma coima de 900.000 euros a uma empresa de 'software' por não adaptar as medidas de segurança e facilitar um ciberataque

O Garante italiano publicou a newsletter n.º 528 de 22 de outubro, em que refere uma resolução adotada em julho contra uma empresa de *software* por ter ignorado durante um ano as recomendações de atualização das medidas de segurança apresentadas tanto por um fornecedor de *software* como pela Agência Nacional de Cibersegurança. A não adoção dessas medidas facilitou um ataque *ransomware* que originou a exfiltração, incluindo a afetação da disponibilidade, de ficheiros que continham dados pessoais de aproximadamente 25.000 titulares, incluindo funcionários, ex-funcionários, candidatos e representantes de empresas com as quais a entidade mantém relações comerciais.

Os dados que foram publicados na *dark web* incluem dados de identificação e de contacto, de acesso, de pagamentos, antecedentes criminais e categorias especiais de dados, como informações de saúde e de filiação sindical.

Além de uma coima de 900.000 de euros, o Garante ordena à sociedade que proceda à análise das vulnerabilidades dos seus sistemas, à mitigação e identificação de tempos de deteção e resposta adequados ao risco.

Empresa sancionada por enviar mais de 200 SMS publicitários a um particular sem o seu consentimento

No dia 3 de dezembro de 2021, um particular apresentou uma reclamação junto da Agência Espanhola de Proteção de Dados contra uma empresa por receber comunicações publicitárias não solicitadas sobre serviços de vidência. A reclamação fundamentava-se em três motivos: receção permanente de chamadas e mensagens publicitárias, inexistência de opções para cancelar a subscrição e ineficácia da sua inscrição na Lista Robinson.

A AEPD verificou que a reclamada tinha enviado 242 SMS à reclamante ao longo de três meses, sem incluir um mecanismo simples e gratuito para se opor ao tratamento, violando assim o artigo 21.º da LSSI. Apesar das tentativas de cancelamento por parte da reclamante, as mensagens continuaram a chegar.

A reclamada alegou que a sua atividade não estava sujeita à LSSI por não ser um serviço de comércio eletrónico e que as SMS respondiam a pedidos do cliente. Também argumentou que a sua atuação não envolvia tratamento de dados pessoais, pois só registava nomes próprios e signos do zodíaco. No entanto, a Agência ignorou estes argumentos por considerar que as mensagens eram comunicações comerciais eletrónicas sujeitas à LSSI.

Na sua resolução de 29 de outubro com a referência N.º: EXP202200418, a AEPD concluiu que a infração era grave e agravada pela sua persistência, aplicando uma coima de 30.010 euros à reclamada.

Um particular é multado por instalar câmaras de vigilância que captavam imagens de áreas privadas

No dia 17 de abril de 2023, um particular apresentou uma reclamação contra outro por instalar um sistema de videovigilância num numa quinta arrendada onde funcionava um clube hípico. O denunciante alegou que as câmaras captavam imagens de áreas arrendadas, como a pista de treino, a casa de banho feminina e o estacionamento, afetando a privacidade de clientes, incluindo menores e pessoas portadoras de deficiência, sem o seu consentimento nem a informação adequada.

O denunciante apresentou provas, como fotografias, um documento notarial e publicações nas redes sociais; e o reclamado, por sua vez, não respondeu ao pedido da Agência para comprovar ações corretivas. Consequentemente, em outubro de 2023, iniciou-se um procedimento sancionador por alegada violação do artigo 6.º, n.º 1 do RGPD, que exige uma base que legitime o tratamento de dados pessoais.

Na sua resolução de 30 de outubro com a referência N.º: EXP202305765, a Agência considerou provado que as câmaras captavam imagens de áreas privadas sem consentimento nem justificação legal. Isto constitui uma infração grave do RGPD e da LOPDGDD, que obriga a limitar a videovigilância para garantir a segurança sem invadir a intimidade de terceiros.

Foi aplicada ao denunciado uma multa de 2.000 euros e foi ordenada a retirada ou a reorientação das câmaras no prazo de um mês para cumprir a regulamentação.

Partido político sancionado por usar no seu programa eleitoral a imagem de um particular sem autorização

No dia 22 de maio de 2023, uma particular apresentou uma reclamação perante a Agência Espanhola de Proteção de Dados contra um partido político de uma autarquia local pela utilização não autorizada da sua imagem no programa eleitoral do partido. A reclamante alegou que, embora tenha tirado uma fotografia durante um ato público em abril de 2023, tinha declarado previamente que não pretendia que a sua imagem fosse utilizada com fins políticos, o que ficou registado numa mensagem de WhatsApp. Apesar desta advertência, a imagem apareceu no programa eleitoral e nas redes sociais do partido.

O denunciado alegou que a imagem tinha carácter institucional e que a sua utilização

fazia parte da promoção de atividades públicas do município. Contudo, a AEPD concluiu que a utilização da imagem no programa eleitoral extravasava o propósito original e não se baseava no consentimento expresso da reclamante, tal como exige o Regulamento Geral de Proteção de Dados (RGPD). A agência considerou que a publicação inicial da imagem pela autarquia local não autorizava a sua reutilização num contexto eleitoral.

Na sua resolução de 31 de outubro com a referência N.º: EXP202308206, a AEPD aplicou uma sanção de 5.000 euros al partido por violação do artigo 6.º, n.º 1 do RGPD, sublinhando a falta de diligência na obtenção de consentimento e o uso indevido de dados pessoais.

AEPD sanciona com 6,5 milhões de euros uma empresa distribuidora de telecomunicações por uma falha de segurança

Na sua resolução ps-00084-2023 a AEPD indefere o recurso de reposição apresentado por uma empresa distribuidora de telecomunicações contra a resolução da AEPD de 27 de dezembro de 2023 que lhe aplicava uma coima no valor total 6,5 milhões de euros pela violação dos artigos 5.º, n.º 1, al. f) e 32.º do Regulamento Geral de Proteção de Dados em relação a uma violação de dados pessoais ocorrida em 2021.

Como consequência da falha provocada pelo *ransomware* Babuk Locker, a confidencialidade de determinados dados pessoais (nome completo, data de nascimento, endereço e correio eletrónico) de aproximadamente 13 milhões de clientes, ex-clientes, fornecedores e funcionários da empresa sancionada ficou comprometida. A AEPD recebeu 211 reclamações de titulares afetados.

Embora a empresa alegasse ter sido vítima de um ciberataque sofisticado, a AEPD determina que as medidas de segurança implementadas pela sociedade eram insuficientes, incumprindo o RGPD. A AEPD também recusa a existência de um concurso de infrações entre os artigos 5.º, n.º 1, al. f) e 32.º do RGPD, considerando que a violação do artigo 32.º ocorre independentemente de ter existido ou não uma falha de confidencialidade, pois o que se sanciona é a falta ou inadequação dessas medidas. Pelo contrário, a violação do artigo 5.º, n.º 1, al. f) do RGPD resulta do facto de não se ter garantido uma segurança adequada através das medidas técnicas e organizativas apropriadas, não só de segurança, mas de todo o tipo.

A denunciada apresentou um recurso contencioso administrativo perante a Audiência Nacional solicitando a suspensão cautelar do pagamento e a confidencialidade de determinados documentos, mas a Audiência indeferiu este pedido.

AEPD sanciona com 200.000 euros uma empresa de telecomunicações pela emissão de duplicados de cartões SIM para terceiros

Na sua resolução ps-00425-2023 a AEPD indefere o recurso de reposição apresentado por uma empresa de telecomunicações contra a resolução da AEPD de 8 de maio de 2024, que aplicava uma coima no valor de 200.000 euros por violação do artigo 6.º, n.º 1 do RGPD, por ter sido realizado um tratamento ilícito dos dados pessoais de um titular em relação à emissão de duplicados de cartões SIM.

A AEPD considerou que a sociedade não agiu diligentemente ao não seguir o procedimento implementado para identificar corretamente os seus clientes, o que originou um tratamento ilícito dos dados pessoais. Embora a AEPD concordasse com o argumento da denunciada de que a emissão de duplicados do cartão SIM não é suficiente para realizar operações bancárias em nome dos titulares, destacou a importância da diligência das operadoras para evitar este tipo de fraudes e violações do RGPD.

Além disso, a AEPD indeferiu o pedido de arquivamento do processo por inexistência de

culpa, assinalando que a sociedade não adotou as medidas necessárias para evitar as tentativas de alteração do endereço de correio eletrónico por via telefónica.

Criador de conteúdos é sancionado com 10.000 euros pela publicação de um vídeo de uma menor a responder a perguntas relativas à sua vida sexual

Os pais da menor denunciaram à polícia a publicação de um vídeo no TikTok e no Instagram por um criador de conteúdos sem o seu consentimento. Esse criador, com milhares de seguidores em várias plataformas, alegou que tinha solicitado aos menores que informassem os seus pais sobre a gravação e, ao não receber qualquer oposição, publicou o vídeo. No entanto, na sua resolução ps-00471-2023 a AEPD concluiu que o tratamento de informação relativa à vida sexual de uma menor, tratando-se de categorias especiais de dados, implica que se verifiquem circunstâncias específicas de acordo com o artigo 9.º, n.º 2 do RGPD, além de uma base de legitimação adequada, nos termos do artigo 6.º, n.º 1 do RGPD. Neste sentido, a AEPD considera que não existiu um consentimento prévio dos progenitores da menor de acordo com os requisitos da regulamentação em matéria de proteção de dados.

Além das violações dos artigos 9.º, n.º 2 e 6.º, n.º 1 do RGPD, a Agência aplicou sanções adicionais por violações dos artigos 5.º, n.º 1, al. c) e 13.º do RGPD, que somam um total de 10.000 euros. Quanto à violação do artigo 5.º, n.º 1, al. c) do RGPD (princípio de minimização de dados), a AEPD refere que a difusão do vídeo da menor nas redes é um tratamento excessivo, uma vez que a notícia também poderia ter sido transmitida sem necessidade de identificar a menor através do vídeo.

AEPD sanciona com 20.000 euros empresa automóvel porque a sua política de 'cookies' não cumpre a regulamentação

Depois de investigar oficiosamente o site de uma empresa automóvel, a AEPD, na sua resolução ps-00284-2024, inicia um processo sancionador contra essa empresa e aplica uma sanção inicial de 20.000 euros pela violação do artigo 22.º, n.º 2 da Lei de Serviços da Sociedade da Informação e de Comércio Eletrónico. A Agência detetou várias deficiências na política de *cookies* da empresa, mais concretamente: (i) a instalação de *cookies* não técnicos (como *cookies* de funcionalidade ou de segmentação) no dispositivo do utilizador quando este acedia ao site pela primeira vez, tendo limpo o equipamento do historial de navegação e *cookies*, e sem ter aceitado novos *cookies* nem realizado qualquer ação sobre a mesma; e (ii) que, embora existindo um mecanismo que permite ao utilizador retirar o consentimento para a utilização dos *cookies* depois de prestado, continua a ser enviada ao servidor informação de *cookies* não técnicos quando deveriam ser eliminados.

Finalmente, a Agência decreta a extinção do processo por pagamento voluntário, pois a entidade denunciada tinha procedido ao pagamento da coima no valor de 12.000 euros, usando as duas reduções previstas no acordo inicial.

AEPD aplica uma sanção de 200.000 euros a uma entidade bancária por realizar um tratamento de dados pessoais sem base legitimadora suficiente

A reclamante tinha sido funcionária do banco e, depois de terminar voluntariamente a sua relação laboral, manteve o seu terminal móvel empresarial para uso pessoal, beneficiando de um programa empresarial nesse sentido. Algum tempo depois da cessação da relação laboral, tendo usado para fins privados o referido telemóvel, este apresentou uma mensagem com a indicação de que estava a ser administrado remotamente pelo banco e que era necessário entrar com a sua conta empresarial para continuar a sua utilização. Depois de entrar em contacto com o banco, a única solução para recuperar a funcionalidade do dispositivo foi a eliminação de todos os

conteúdos do dispositivo para o repor no seu estado original de fábrica. Isso implicou a perda de informação estritamente pessoal e privada da reclamante.

Na sequência destes acontecimentos, a AEPD, conforme acima se indica, considera que o banco realizou o tratamento dos dados pessoais da reclamante sem fundamento de legitimidade, uma vez que já não mantinha com ela qualquer relação laboral, nem existia qualquer outra base que legitimasse o tratamento.

No processo sancionador EXP202303478, a AEPD aplica uma sanção de 200.000 euros à entidade bancária (valor reduzido a 120.000 euros pelo pagamento voluntário) por efetuar um tratamento de dados pessoais sem fundamento legitimador suficiente, nos termos do artigo 6.º do RGPD.

Três empresas sancionadas pela utilização de 'cookies' de Google Analytics

Nos processos independentes EXP202315694 (PA/00061/2023), EXP202315693 (PA/00060/2023) e EXP202203580 (PA/00053/2023), a AEPD adota decisões semelhantes em relação à utilização de *cookies* e tecnologias similares nos sites de três empresas. Mais concretamente, a análise da AEPD centra-se na utilização de *cookies* de Google Analytics por estas entidades, com a consequente realização de transferências internacionais que tal implica.

Depois de analisar a utilização destas tecnologias pelos investigados, a AEPD considera que, de facto, estava a ser realizado, por sua vez, um tratamento de dados pessoais em relação aos quais aqueles atuavam como responsáveis. Além disso, considera que: (i) não se encontra devidamente provado que os dados pessoais dos titulares foram anonimizados antes do seu acesso pela Google; e (ii) atendendo à documentação disponível, a Google poderia estar a aceder a essa informação a partir dos EUA, ou seja, de fora do Espaço Económico Europeu. Consequentemente, a utilização destas tecnologias envolvia uma transferência de dados pessoais para os EUA.

Neste sentido, a AEPD resolve que, aquando dos factos (anteriores ao estabelecimento do novo *framework* para a transferência de dados pessoais do Espaço Económico Europeu para os EUA, e posteriores ao acórdão do caso Schrems II que anulou o *privacy shield*), essa transferência internacional não estava devidamente regularizada ao abrigo de nenhum dos mecanismos previstos pelo RGPD, sem que tenham sido implementadas garantias suficientes no respetivo desenvolvimento. Por isso, a AEPD considera que as entidades investigadas não cumpriram a regulamentação aplicável, o que suscita a aplicação de um alerta a estas três entidades.

4. Sentenças

O TJUE aborda a legalidade do tratamento de dados sensíveis pela Meta Platforms no caso Schrems

O acórdão do Tribunal de Justiça no processo C-446/21 | Schrems (Comunicação de dados ao público em geral) decorre da denúncia apresentada pelo Sr. Maximilian Schrems perante os órgãos jurisdicionais austríacos, em que argumenta que houve um tratamento ilícito dos seus dados pessoais - entre outros, dados relativos à sua orientação sexual - pela Meta Platforms Ireland no âmbito da rede social Facebook.

A Meta Platforms recolhe dados pessoais dos utilizadores do Facebook relativos às atividades que estes realizam tanto na referida rede social como fora dela (por exemplo, dados relativos à consulta da plataforma online, de sites e de aplicações de terceiros). Para isso, a Meta Platforms utiliza *cookies*, *social plug-ins* e píxeles de seguimento inseridos nos sites em causa. Além disso, a Meta Platforms também pode identificar o interesse que o utilizador pode ter em temas sensíveis, como a orientação sexual, o que permite dirigir-lhe publicidade específica a este propósito.

Por isso, coloca-se a questão de saber se o Sr. Schrems tornou manifestamente públicos dados pessoais sensíveis que lhe dizem respeito ao ter comunicado numa mesa redonda aberta ao público a sua condição de homossexual, autorizando com isso o tratamento desses dados nos termos do Regulamento Geral de Proteção de Dados (RGPD).

Neste contexto, o Supremo Tribunal Cível e Penal austríaco solicitou ao TJUE que interprete o RGPD.

Em primeiro lugar, o TJUE responde que o princípio de minimização de dados - estabelecido no RGPD - opõe-se a que todos os dados pessoais que um responsável pelo tratamento (como o operador de uma plataforma de rede social online) tenha obtido do titular ou de terceiros e que tenham sido recolhidos tanto nessa plataforma como fora desta, sejam agregados, analisados e tratados para propor publicidade específica, sem limitação temporal e sem distinção em função da natureza desses dados.

Em segundo lugar, de acordo com o TJUE, não se exclui que, através da sua declaração durante o debate em causa, o Sr. Schrems tenha tornado manifestamente pública a sua orientação sexual, mas determina que cabe ao Supremo Tribunal Cível e Penal austríaco avaliá-lo.

O RGPD não se opõe a uma regulação nacional que permita recorrer de uma violação da regulamentação de proteção de dados por parte de uma empresa concorrente

O Supremo Tribunal Cível e Penal alemão, que deve resolver o litígio entre dois farmacêuticos concorrentes, solicita ao TJUE que interprete o RGPD. No acórdão relativo a este processo (C-21/23 | Lindenapotheke), o TJUE declara que o RGPD não se opõe a uma regulamentação nacional que permita aos concorrentes do alegado violador da regulamentação em matéria de proteção de dados pessoais impugnar judicialmente essa infração como prática comercial desleal proibida. Essa possibilidade de recurso dos concorrentes acresce aos poderes de intervenção das autoridades de controlo responsáveis por supervisionar e zelar pelo cumprimento do RGPD, assim como às possibilidades de recurso dos titulares, estabelecidas naquele regulamento.

Além disso, considera que constituem dados relativos à saúde, no sentido do RGPD, as informações disponibilizadas pelos clientes aquando da compra pela internet de medicamentos reservados às farmácias, mesmo quando a venda destes não esteja sujeita a receita médica. Por isso, o vendedor deve informar estes clientes, de modo exato, completo e facilmente compreensível, das características e fins específicos do tratamento desses dados e pedir o seu consentimento explícito para tal tratamento.

O TJUE pronuncia-se sobre a tentativa de acesso aos dados pessoais armazenados num telemóvel

No processo C-548/21 | Bezirkshauptmannschaft Landeck, a polícia austríaca apreende um dispositivo móvel no âmbito de uma investigação relacionada com o controlo de drogas e tenta aceder (sem sucesso) aos dados do referido dispositivo sem informar o titular e sem ter autorização do juiz ou do Ministério Público. Por sua vez, o titular impugna perante os tribunais austríacos a apreensão, tendo conhecimento das tentativas de acesso através do desbloqueio durante o próprio processo judicial.

Neste contexto, o órgão jurisdicional austríaco pergunta ao TJUE se uma norma nacional que permita à polícia atuar deste modo está conforme a norma da UE. A este propósito, no seu acórdão o TJUE refere que:

a. a norma da UE (neste caso o RGPD) não só se aplica no caso de se aceder com sucesso aos dados pessoais contidos num telemóvel, como também às tentativas de aceder a eles.

b. o acesso a todos os dados contidos num telemóvel pode constituir uma interferência grave, até especialmente grave, nos direitos fundamentais do titular.

c. para evitar uma limitação injustificada dos poderes de investigação das autoridades competentes, essa interferência é permitida desde que o legislador nacional defina de forma suficientemente precisa os elementos que devem ser tidos em conta para que possa ter lugar; em particular, a natureza ou categorias de infrações que podem estar em causa.

d. o acesso também deve estar sujeito a controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, exceto em casos de urgência devidamente justificados, desde que seja garantido um justo equilíbrio dos interesses legítimos envolvidos.

e. o titular deverá ser informado dos motivos que justificam a autorização de acesso, quando essa comunicação não seja suscetível de prejudicar as investigações.

TJUE pronuncia-se sobre a comunicação de dados pessoais com fins promocionais, a troco de uma remuneração

No processo C-621/22, uma associação desportiva foi sancionada pela autoridade de controlo dos Países Baixos por ter divulgado dados pessoais dos seus membros a dois dos seus patrocinadores com fins promocionais, sem dispor de qualquer base legal para o efeito. Assim, a associação recorreu da resolução para os tribunais neerlandeses, alegando que a divulgação dos referidos dados se baseou num interesse legítimo, no sentido do artigo 6.º, n.º 1, al. f) do RGPD, consistindo, por um lado, na criação de um forte vínculo entre a referida associação e os seus membros e, por outro lado, em poder proporcionar valor acrescentado aos seus associados sob a forma de descontos e ofertas.

Neste contexto, o Tribunal neerlandês pergunta ao TJUE se é possível justificar, com base no artigo 6.º, n.º 1, al. f) do RGPD, a comunicação, a troco de remuneração, dos dados pessoais dos seus membros aos patrocinadores da referida associação com fins promocionais.

A este propósito, no seu acórdão o TJUE não exclui que um interesse comercial do responsável pelo tratamento, que consiste na comunicação de dados pessoais para fins promocionais, possa ser considerado um interesse legítimo no sentido do artigo 6.º, n.º 1, al. f) do RGPD, desde que (i) o alegado interesse legítimo seja lícito e (ii) o responsável pelo tratamento cumpra as restantes obrigações do RGPD (por exemplo, o dever de informar os titulares sobre o interesse prosseguido). Lembra ainda que o considerando 47 do RGPD prevê, a título de exemplo, os fins de marketing direto como interesses legítimos que um responsável pode perseguir.

Além disso, o TJUE refere-se aos restantes requisitos cumulativos que devem ser apreciados para determinar se esse interesse prevaleceria sobre os direitos e liberdades dos titulares, assim como a necessidade de analisar se esse interesse poderia ser razoavelmente alcançado com a mesma eficácia através de outros meios menos restritivos dos direitos e liberdades dos titulares. Neste sentido, o TJUE sugere que a associação poderia ter alcançado o alegado interesse com igual eficácia se tivesse informado e consultado previamente os titulares sobre a comunicação dos seus dados a terceiros.

Por último, o TJUE salienta que, entre os interesses que deveriam ter sido ponderados, estão as expectativas razoáveis dos titulares de que os seus dados fossem divulgados a título oneroso aos patrocinadores da associação para fins promocionais. Contudo, neste caso, o TJUE tem dúvidas de que esta expectativa possa existir.

Supremo Tribunal confirma a sanção de 200.000 euros aplicada pela AEPD a uma empresa de serviços de telecomunicações

O Supremo, no seu acórdão n.º 1569/2024 de 8 de outubro de 2024, indefere o recurso de cassação apresentado por uma empresa de serviços de telecomunicações e confirma a sanção de 200.000 euros que lhe foi imposta pela AEPD. A sanção deveu-se ao facto de a empresa não adotar medidas de segurança adequadas para evitar a geração fraudulenta de cartões SIM duplicados, o que permitiu o acesso não autorizado aos dados pessoais dos seus clientes, violando assim o artigo 5.º, n.º 1, al. f) do RGPD.

A empresa denunciada alegou que a conduta infratora se deveria enquadrar apenas no artigo 32.º do RGPD e não no artigo 5.º, n.º 1, al. f), pois, ao centrar-se nas medidas técnicas e organizativas de segurança, é mais preciso, devendo, por isso, aplicar-se exclusivamente nos casos de medidas de proteção insuficientes.

No entanto, o Supremo considerou que o artigo 5.º, n.º 1, al. f) do RGPD não é apenas um preceito geral, mas também impõe uma obrigação concreta de proporcionar uma segurança adequada dos dados pessoais, mesmo contra o tratamento não autorizado ou ilícito mediante a adoção de medidas de segurança técnicas ou organizativas apropriadas. O tribunal sublinha que, em caso algum, o artigo 5.º, n.º 1, al. f) pretende afastar a aplicação do artigo 32.º, mas antes que este último venha complementar e desenvolver a obrigação estabelecida no artigo 5.º.

Supremo Tribunal permite que a AEPD reveja em pormenor as políticas de privacidade de uma entidade bancária no âmbito de um procedimento sancionatório, anulando a decisão anterior da AN

No acórdão 1792/2024 de 11 de novembro do Rec. 2960/2023, o Terceiro Juízo de Contencioso-Administrativo, 3.ª Secção, do Supremo Tribunal deu provimento ao recurso da AEPD contra a resolução anterior da Audiência Nacional que anulava as sanções impostas pela AEPD contra uma entidade bancária. Este procedimento perante a AEPD resultou de uma série de reclamações da entidade bancária relacionadas com o tratamento dos seus dados pessoais para fins comerciais.

Mais concretamente, neste caso, e apreciando o recurso da entidade bancária contra a resolução da AEPD, a AN considerou que esta não podia "alargar" o objeto do procedimento sancionatório à revisão geral da política de privacidade da entidade bancária, uma vez que tal implicaria a realização de uma espécie de processo geral contra a reclamada a partir de um número limitado de reclamações sobre factos concretos. No entanto, o TS considera que a AEPD não violou em caso algum o princípio da proibição da arbitrariedade ou da segurança jurídica, tanto mais que a política de privacidade revista teve uma relação direta com os casos analisados.

Com esta resolução, o TS abre as portas a que a AEPD possa analisar detalhadamente o estado de conformidade normativa dos responsáveis pelo tratamento, especialmente em relação às suas políticas de privacidade em sentido lato, sem ficar estritamente condicionada pelo conteúdo das reclamações recebidas, e sempre de acordo com os princípios e regras que regem o procedimento sancionatório e a atuação das autoridades públicas.

Supremo Tribunal decide um recurso de cassação apresentado contra a Google sobre a ponderação entre o direito à proteção de dados pessoais e a publicidade das decisões judiciais

O recurso foi interposto solicitando a desindexação de determinados links do motor de busca da Google que direcionavam para uma decisão do Supremo Tribunal de Justiça da Colômbia. A sentença em causa versava sobre um conflito familiar relacionado com o regime de visitas de um menor. Argumentava-se que a publicação da referida decisão violava o direito à proteção dos dados pessoais e afetava a honra, a privacidade e a imagem do recorrente.

No acórdão 1775/2024 o Terceiro Juízo de Contencioso-Administrativo, 3.ª Secção, do Supremo Tribunal indeferiu o recurso, argumentando que o direito à proteção de dados pessoais não é absoluto e deve ser ponderado com outros direitos em conflito, neste caso, o dever de publicidade das decisões judiciais. A decisão sublinha que a publicidade das decisões judiciais é um bem jurídico de interesse público, especialmente quando se trata de documentos oficiais publicados por uma autoridade judicial no exercício das suas funções. O tribunal salientou ainda que a informação constante do acórdão publicado não incluía dados considerados relevantes para a exclusão da identidade nos termos da Deliberação do Plenário do Tribunal Constitucional. Além disso, referiu que não foram fornecidas provas suficientes para demonstrar que as informações eram imprecisas ou obsoletas. Por tudo isto, o Supremo Tribunal concluiu que a ponderação de direitos efetuada

pela decisão impugnada foi correcta e conforme ao direito, prevalecendo, neste caso, o interesse público na difusão da decisão judicial sobre o direito à protecção de dados pessoais.

5. Atualidade

Peru: Publicado o novo Regulamento da Lei de Proteção de Dados Pessoais

O novo Regulamento da Lei de Proteção de Dados Pessoais no Peru, publicado a 30 de novembro de 2024, introduz alterações significativas para reforçar a segurança e o tratamento de dados pessoais, respondendo às necessidades de um ambiente cada vez mais digital. Entre as novidades, é desenvolvido um novo procedimento de notificação de incidentes de segurança no prazo de 48 horas, que envolve a informação tanto à Autoridade Nacional de Proteção de Dados Pessoais como aos titulares afetados. Além disso, é introduzida a figura do Encarregado de Dados Pessoais, responsável interno que garante o cumprimento dos regulamentos em empresas públicas e privadas com tratamento significativo de dados especialmente sensíveis.

O regulamento reforça ainda os direitos dos cidadãos através da implementação de medidas como a portabilidade dos dados, permitindo aos titulares dos dados transferir os seus dados entre diferentes responsáveis pelo tratamento. De igual modo, as sanções são reforçadas para quem não cumpre os regulamentos, incluindo o atraso na resposta aos pedidos de direitos ARCO ou a falta de designação de um encarregado dos dados. Estas disposições procuram garantir uma maior transparência e segurança na gestão da informação, adaptando-se aos padrões internacionais e protegendo os direitos digitais num ambiente globalizado.

Com a entrada em vigor deste novo Regulamento, prevista para 30 de março de 2025, será revogado o regulamento anterior, em vigor desde 2013.

Pode aceder a mais pormenores sobre este regulamento neste link.

O registo de viajantes: Desafios e Polémicas do Real Decreto 933/2021

No passado dia 2 de dezembro de 2024 foi efetivamente aplicado o Real Decreto 933/2021, que obriga as empresas de alojamento, aluguer de veículos e operadores turísticos a recolher, conservar e transmitir dados sobre os seus clientes às autoridades espanholas. Esta regulamentação, que tem gerado um intenso debate tanto a nível nacional como internacional, coloca inúmeros desafios em matéria de privacidade.

E tal acontece porque o Real Decreto 933/2021 não só alarga o âmbito de aplicação das suas obrigações a novos intervenientes no setor do turismo, como também aumenta significativamente a quantidade de dados pessoais que devem ser recolhidos e transmitidos às autoridades. Tudo isto levanta inúmeras dúvidas e preocupações jurídicas

sobre, entre outros, a proporcionalidade e previsibilidade destas obrigações. As empresas sujeitas ao Real Decreto 933/2021 podem cumprir as suas obrigações sem violar os direitos de proteção de dados dos viajantes? Que implicações tem a aplicação efetiva deste Real Decreto para o setor do turismo e como se alinham as obrigações nele previstas com a regulamentação de proteção de dados aplicável? Descubra os pormenores e as polémicas neste artigo**.**

A ONU publica o seu relatório final 'Governação da IA para a Humanidade'

A Organização das Nações Unidas (ONU) publicou o seu relatório final intitulado 'Governação da IA para a Humanidade', em que estabelece a necessidade de dispor de um sistema de governação global de IA sustentada num enfoque integral e inclusivo em relação aos âmbitos político, económico, social, etc.

O relatório destaca que as atuais iniciativas de governação da IA são afetadas por (i) lacunas de representação: a maioria das iniciativas de governação não são totalmente representativas; (i) lacunas de coordenação: existe o risco de incompatibilidade entre iniciativas de diferentes regiões; e (iii) lacunas de implementação: é necessário garantir que os compromissos de boa governação se traduzam em resultados tangíveis.

Para reverter os efeitos destas lacunas, a ONU apresenta sete recomendações que estão resumidas no relatório final e se estabelecem em torno de quatro propósitos:

A ONU termina o relatório com um apelo à ação para se atingir um cenário de governação da Iainclusivo e capacitador para as pessoas, as comunidades e os países do mundo inteiro.

Publicada a versão provisória da Orientação do CEPD para a utilização do interesse legítimo como base legitimadora

Com data de outubro de 2024, o Comité Europeu para a Proteção de Dados (CEPD) publicou a versão provisória da Orientação 1/2024 sobre o tratamento de dados pessoais baseado no artigo 6.º, n.º 1, al. f) do RGPD (interesse legítimo), encontrando-se agora em fase de consulta pública. Estas orientação, que atualiza o Parecer 06/2014 do Grupo de Trabalho 29, reúne os principais critérios interpretativos, jurisprudência do TJUE e exemplos que devem ser considerados ao utilizar essa base legitimadora.

Esta orientação aprofunda a utilização do interesse legítimo para fins de marketing direto, indica os casos em que entra em jogo o interesse legítimo de um terceiro e desenvolve o conceito de expectativa razoável do titular. No entanto, deverá aguardar-se pela versão final do documento para se tirarem conclusões definitivas.

Publicado o Parecer 22/2024 sobre determinadas obrigações decorrentes da utilização de subcontratante(s) subcontratante(s) ulterior(es)

Com data de 7 de outubro de 2024, o CEPD adotou o parecer 22/2024 que delimita as obrigações dos responsáveis ao recorrer a subcontratantes (e subcontratantes ulteriores) para o tratamento, dando assim resposta às questões colocadas pela autoridade de proteção de dados dinamarquesa.

Como conclusão geral, o responsável pelo tratamento deve ter sempre identificados todos os subcontratantes (ulteriores) que acedam aos dados pessoais e verificar se todos cumprem as medidas de segurança exigidas pelo RGPD.

No entanto, o alcance desta verificação dependerá do risco envolvido no tratamento em causa. Além disso, a CEPD valida que o contrato de subcontratação permita ao subcontratante não seguir as instruções do responsável se estas contrariarem a regulamentação extra-europeia, desde que essa atuação não entre em conflito com o cumprimento do RGPD.

Realizada a quarta Mesa Redonda das Autoridades de Proteção de Dados do G7

De 9 a 11 de outubro deste ano, realizou-se a quarta edição da Mesa Redonda das Autoridades de Proteção de Dados do G7 em Roma, em que participaram as autoridades do Canadá, França, Alemanha, Japão, Reino Unido, EUA, o Comité Europeu de Proteção de Dados (CEPD) e a Autoridade Europeia para a Proteção de Dados (EDPS).

As discussões centraram-se nos seguintes três tópicos principais: o *Data Free Flow with trust* (DFFT), o impacto das tecnologias emergentes e a cooperação na aplicação da regulamentação, tudo numa perspetiva da utilização crescente da inteligência artificial (IA).

Os principais resultados foram uma declaração sobre o papel das autoridades para garantir que as tecnologias de IA são fiáveis e cumprem os regulamentos de proteção de dados, uma declaração sobre a IA e as crianças e uma declaração sobre a importância de existirem mecanismos robustos para transferências internacionais de dados.

O CEPD lança um novo guia sobre o alcance técnico do art.º 5.º, n. 3 da Diretiva ePrivacy

O Comité Europeu de Proteção de Dados (CEPD) publicou novas orientações em que se pronuncia sobre a aplicação do artigo 5.º, n.º 3 da Diretiva ePrivacy a novas ferramentas de seguimento, que ampliam o Parecer 9/2014 do GT29 sobre *fingerprinting* ou pegada digital de um dispositivo.

Estas orientações procuram identificar e analisar três dos elementos-chave para a aplicabilidade do artigo 5.º, n.º 3 da Diretiva: (i) informação, (ii) equipamentos terminais e (iii) acesso ou armazenamento. As ambiguidades quanto ao âmbito de aplicação do referido artigo têm gerado grande polémica e, por isso, exigem estas novas orientações, que asseguram também a implementação das conclusões técnicas a que se refere a expressão "armazenar informação ou obter acesso a informação armazenada no terminal de um assinante ou utilizador."

Estas novas orientações também abordam uma lista não exaustiva de casos de utilização específicos para a tecnologia de seguimento, como o seguimento por IP ou o seguimento por URL.

Terminou o prazo para transpor a directiva SRI 2 para o direito interno sem que Espanha o tivesse feito

A Diretiva SRI 2, relativa às medidas para garantir um elevado nível de cibersegurança, foi formalmente aprovada em novembro de 2022, publicada no Jornal Oficial da UE (JOUE) a 27 de dezembro de 2022, e entrou em vigor em 16 de janeiro de 2023. Os Estados-Membros deveriam adotar e publicar as medidas necessárias para cumprir as disposições da diretiva antes de 17 de outubro de 2024.

No entanto, este prazo para os Estados-Membros transporem a diretiva NIS2 para o seu direito interno esgotou-se sem que Espanha tivesse publicado o quadro legislativo definitivo para a adaptar especificamente. Até ao momento, apenas a Bélgica, a Croácia e a Hungria publicaram a transposição. Embora as recomendações da directiva sejam claras e seja agora possível iniciar o processo de adaptação para adoptar medidas básicas de cibersegurança (como a gestão de incidentes, análise de risco e segurança da cadeia de abastecimento), o legislador espanhol deverá avançar com um anteprojecto assim que possível para evitar ser sancionado.

AEPD apresenta uma nova metodologia para a modelação de ameaças para a privacidade e a proteção de dados

A AEPD emitiu uma nota técnica para apresentar a LIINE4DU 1.0: uma nova

metodologia para a modelação de ameaças para a privacidade e a proteção de dados.

O único método de modelação de ameaças para a privacidade deste tipo que foi publicado e que é utilizado amplamente é o LINDDUN (*Linking, Identifying, Non-repudiation, Detecting, Data disclosure, Unawareness y Non-compliance*).

A AEPD considera que, embora o LINDDUN seja uma estrutura robusta para analisar ameaças à privacidade, tem desvantagens quando é utilizado especificamente para apoiar o cumprimento do RGPD e realizar uma avaliação de impacto relativa à proteção de dados. O LINDDUN centra-se, principalmente, nas ameaças técnicas, sem abordar na mesma medida os aspetos organizacionais e processuais do cumprimento do RGPD.

Por isso, a AEPD está a trabalhar num novo quadro LIINE4DU (*Linking, Identifying, Inaccuracy, Non-repudiation, Exclusion, Detecting, Data Breach, Deception, Data Disclosure, Unawareness and Unintervenability*) que se centre na protecção dos direitos e liberdades das pessoas e no cumprimento do RGPD.

Publicado um relatório sobre o artigo 36.º da Decisão 2007/533/JAI relativa ao estabelecimento, funcionamento e utilização do SIS II

O Comité de Supervisão Coordenada do SIS II emitiu um relatório sobre os requisitos para a ativação dos alertas do artigo 36.º do SIS II no âmbito da atividade de inspeção do Sistema de Informação Schengen, devido ao aumento deste tipo de alertas na Europa. Recordemos que o SIS foi criado como contrapeso à abertura das fronteiras entre os Estados-Membros do espaço Schengen, e contém alertas emitidos por esses Estados-Membros para a repressão de crimes e a prevenção de ameaças à segurança pública.

30 autoridades de controlo da proteção de dados de 19 Estados-Membros participaram e contribuíram com as suas opiniões para a elaboração do relatório. O Comité conseguiu verificar que existem diferenças entre os diversos Estados, razão pela qual inclui um conjunto de recomendações às autoridades que iniciam estes alertas, centradas principalmente em verificar se (i) todos os requisitos legais do alerta foram cumpridos, (ii) o caso e a decisão de emitir um alerta estão suficientemente documentados pelos órgãos responsáveis, (iii) apenas estão incluídos os dados necessários para emitir o alerta, e (iv) foram seguidos os procedimentos nacionais.

Costa Rica: Primeiro país do mundo a utilizar inteligência artificial para criar a sua estratégia de marca país

A Costa Rica tornou-se o primeiro país do mundo a utilizar inteligência artificial para criar a sua estratégia de marca país, denominada "Esential COSTA RICA". Esta estratégia procura planear como será o país em 2035, destacando-se o seu compromisso com o ambiente e as alterações climáticas.

Para desenvolver esta estratégia, a Costa Rica trabalhou com a Bloom Consulting e recolheu informação de diversas fontes, como estudos sobre a forma como o país é percebido e documentos sobre sustentabilidade. Recorrendo à IA, analisaram estes dados para compreender melhor como é vista a Costa Rica e que tendências podem influenciar a sua imagem no futuro.

Graças à IA, conseguiram identificar áreas onde podem melhorar a sua presença no mundo e antecipar a forma como os meios de comunicação social falarão sobre o país. Os principais temas da estratégia são a sustentabilidade e a luta contra as alterações climáticas, com a intenção de posicionar a Costa Rica como líder nestas questões a nível global.

A diretora da "Esencial COSTA RICA" refere que o país já está a trabalhar em atividades com empresas para fortalecer a sua imagem e promover a sustentabilidade.

CEPD e Comissão Europeia publicam o relatório sobre o primeiro ano de implementação do 'Data Privacy Framework' entre a UE e os EUA

Tanto a Comissão Europeia como o CEPD avaliaram em relatórios separados (de 9 de outubro e 4 de novembro, respetivamente) se o *Data Privacy Framework* entre a UE e os EUA (DPF) garante um nível adequado de proteção de dados para os cidadãos da União Europeia quando os seus dados pessoais são transferidos para os EUA. As duas instituições concluíram que as autoridades norte-americanas desenvolveram esforços e cooperaram na implementação das estruturas e procedimentos necessários ao funcionamento eficaz do DPF e nos vários progressos alcançados desde a sua aprovação.

Foi salientada a necessidade de as autoridades dos EUA iniciarem proativamente atividades de controlo para garantir a conformidade com os princípios da DPF por parte das empresas certificadas. Além disso, foi sugerido que fossem desenvolvidas orientações comuns adicionais entre as autoridades dos EUA e da UE sobre aspetos-chave do DFP, como a especificação dos requisitos que as empresas certificadas devem cumprir.

A Comissão Europeia indica que será realizada uma nova revisão periódica dentro de três anos para avaliar o progresso e a aplicação prática dos novos regulamentos que estão a ser desenvolvidos nos EUA em matéria de privacidade e segurança nacional.

Apresentadas as primeiras sete propostas de fábricas de IA na UE

Entre os principais objetivos da Comissão Europeia está a criação das primeiras fábricas de inteligência artificial no início de 2025. Estas fábricas destinam-se a criar um ecossistema europeu próspero para treinar modelos avançados de IA e desenvolver soluções de IA em torno de supercomputadores novos e existentes no território da UE. Além disso, integrarão elementos essenciais para o sucesso da IA, como o poder computacional, os dados e o talento.

Ao mesmo tempo que promovem a inovação em IA em toda a União, estas fábricas visam fomentar a colaboração e o desenvolvimento neste domínio, oferecendo recursos de ponta às startups, à indústria e aos investigadores europeus de IA em diferentes setores-chave, como os cuidados de saúde, a energia, a indústria transformadora ou a meteorologia.

A este propósito, a Comissão analisou sete propostas apresentadas por 15 Estados-Membros da UE, entre eles Espanha e dois Estados participantes associados (Noruega e Turquia). Estas propostas apresentadas no âmbito da Empresa Comum EuroHPC, que gere o concurso anunciado em setembro de 2024, serão analisadas por um grupo independente de peritos. A Empresa Comum EuroHPC deverá anunciar a seleção das primeiras fábricas de IA em dezembro de 2024 e colocá-las em funcionamento pouco depois.

Meta lança um novo modelo de publicidade

A Meta lançou um novo modelo nas suas aplicações, com o qual, entre outras novidades, oferece a possibilidade de (i) efetuar um pagamento para poder utilizar as suas aplicações sem ser alvo de publicidade personalizada; (ii) continuar a utilizar as aplicações gratuitamente, para que os dados do utilizador possam ser utilizados para lhe enviar anúncios personalizados; ou (ii) utilizar as aplicações gratuitamente, recebendo publicidade personalizada, mas de forma mais limitada e baseada em informação menos detalhada.

Esta terceira possibilidade é a nova opção incluída no modelo e, de acordo com a informação divulgada pela própria entidade, consistiria em produzir impactos publicitários principalmente com base na informação contextual de cada sessão do utilizador. Ou

seja, personalizar os anúncios com base no conteúdo visualizado por cada interessado numa sessão de utilização da aplicação.

O novo modelo gerou múltiplas reações no setor e não deixa de gerar alguma polémica. O seu funcionamento e implementação devem ser analisados detalhadamente para avaliar todas as suas implicações do ponto de vista da regulamentação aplicável e das orientações do CEPD relativamente a este tipo de tratamento de dados pessoais.

Aprovados novos requisitos de cibersegurança para produtos com elementos digitais

Em 20 de novembro foi publicado no Jornal Oficial da UE o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.° 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência).

Este novo regulamento estabelece requisitos de cibersegurança para produtos com elementos digitais. Entrará em vigor a 10 de dezembro de 2024 e será aplicável a partir de 11 de dezembro de 2027, com obrigações de notificação a partir de 11 de setembro de 2026.

Este regime normativo destina-se a garantir que produtos como câmaras domésticas, frigoríficos, televisores e brinquedos conectados sejam seguros antes de serem introduzidos no mercado. Este regulamento procura colmatar as lacunas do atual quadro legislativo em matéria de cibersegurança, clarificar as ligações com a referida legislação e obter uma maior coerência, garantindo que os produtos com componentes digitais são seguros em toda a cadeia de abastecimento e durante o seu ciclo de vida.

O regulamento aplicar-se-á a todos os produtos ligados direta ou indiretamente a outro dispositivo ou rede, com algumas exceções para produtos que já tenham requisitos de cibersegurança estabelecidos noutras normas da UE, como produtos médicos, aeronáuticos e automóveis.

O novo regime normativo permitirá também aos consumidores ter em conta a cibersegurança na escolha e utilização de produtos com elementos digitais, uma vez que estabelece obrigações para que os fabricantes comuniquem estas características, facilitando a escolha de produtos de *hardware* e *software* que cumpram os requisitos adequados de cibersegurança.

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

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

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

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

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

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

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

Franco Muschi
Sócio · Lima
franco.muschi@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: