MACEDO VITORINO

BREVES NOTAS SOBRE O ATUAL PONTO DA SITUAÇÃO E DESAFIOS

RGPD, TRÊS ANOS DEPOIS

MACEDO VITORINO

ÍNDICE

INTRODUÇÃO

O dia 25 de maio de 2018, data que assinala a aplicação do Regulamento Geral de Proteção de Dados (RGPD) na União Europeia (UE), constitui um importante marco para a privacidade e proteção de dados pessoais. Desde então, passaram três anos, que acrescem aos dois anos de vigência do RGPD e de preparação para a sua aplicação.

É, por isso, inevitável, não só assinalar a data (que também é assinalada por ocasião do Dia da Proteção de Dados, a 29 de janeiro de cada ano), como fazer um ponto da situação da aplicação do RGPD na UE e em Portugal.

O último ano foi um ano *sui generis*, marcado pela pandemia Covid-19 e pelos desafios que esta trouxe para a privacidade e proteção de dados. Estes desafios fizeram sobretudo sentir-se no âmbito do tratamento de dados de saúde e da vida privada; em contexto de teletrabalho e de aulas online com a utilização massiva de plataformas informáticas como o Teams, Zoom, Webex, Google; ao nível da cibersegurança com um aumento dos ataques cibernéticos; no comércio eletrónico (que ganhou uma nova dinâmica); no maior uso das redes sociais (e uso crescente de novas redes sociais) e na publicidade a estas associada.

A estes desafios (não previsíveis) acrescem ainda outros associados a tecnologias de "blockchain", reconhecimento facial e de voz, mineração de informação, inteligência artificial, que, segundo o pai do RGPD, Axel Voss, o RGPD não está preparado para acompanhar, devendo ser revisto. Embora esta opinião não reúna consenso, parece ser, todavia, inquestionável que será necessária uma aplicação rigorosa e eficaz do RGPD sobretudo nos domínios da publicidade em linha, do microdirecionamento e da definição algorítmica de perfis, da classificação, disseminação e amplificação de conteúdos nas plataformas digitais, em empresas integradas e outros serviços digitais. Estes serão certamente os desafios mais próximos.

UM FUNDAMENTO JURÍDICO PARA CADA FINALIDADE DE TRATAMENTO

Todos os fundamentos de licitude são válidos; não há uma hierarquia, mas só é possível utilizar um fundamento para cada finalidade de tratamento. É ainda necessário referir a que operação específica de tratamento cada fundamento se aplica.

Os fundamentos que legitimam as operações de tratamento de dados são: (i) o consentimento do titular dos dados; (ii) a execução de um contrato ou de diligências pré-contratuais; (iii) o cumprimento de obrigações jurídicas; (iv) o interesse vital do titular dos dados; (v) o exercício de funções de interesse público ou o exercício de autoridade pública; e (vi) o interesse legítimo.

Quando esteja em causa o tratamento de categorias especiais de dados (origem racial ou étnica, convicções religiosas, dados genéticos, dados biométricos, dados relativos à saúde), é ainda necessário identificar uma condição específica de entre as previstas no artigo 9.º do RGPD, por exemplo, consentimento explícito, cumprimento de obrigações em matéria de legislação laboral, interesse público no domínio da saúde pública.

Todos os fundamentos são igualmente válidos (desde que aplicáveis).

Não existe um nível hierárquico entre os fundamentos jurídicos.

A mesma operação de tratamento pode basear-se em mais do que um fundamento. Por exemplo, os mesmos dados pessoais podem ser recolhidos para a execução de um contrato e, com base em consentimento, para efeitos de marketing direto. Só é, todavia, possível utilizar um fundamento para cada finalidade de tratamento. Se determinados dados pessoais são recolhidos, com base em consentimento, para a finalidade de marketing direto, não é possível recorrer ao interesse legítimo para justificar a mesma finalidade.

Esta ainda é uma prática comum e que deve ser revista.

Também é comum e deve ser melhorado o texto das políticas de privacidade, que usualmente mencionam todos os fundamentos, sem referir a que operação específica de tratamento cada fundamento se aplica.

É necessário especificar o fundamento aplicável às operações de tratamento. Caso contrário, não é possível saber que fundamentos legitimam que finalidades e cumprir, de forma cabal, o RGPD, em particular os fundamentos de licitude e o dever de informação.

O CONSENTIMENTO LIVRE E O TESTE DE EQUILÍBRIO DO INTERESSE LEGÍTIMO

É ainda comum o consentimento ficar sujeito a descontos ou ofertas comerciais ou ser condição do acesso a um serviço. Continuam também a existir vários equívocos quanto ao uso do «interesse legítimo» e sem o necessário teste de equilíbrio.

A versão em língua portuguesa do conceito de consentimento (artigo 4.º ponto 11) do RGPD), deixou de conter a expressão explícita, com a publicação da declaração de retificação de 4 de março de 2021.

«Consentimento» é uma manifestação de vontade livre, específica, informada e inequívoca do titular dos dados. Isto não significa que o consentimento não tenha que ser explícito em determinadas situações, como acontece para o tratamento de categorias especiais de dados.

É ainda comum o consentimento ser posto em causa por práticas pouco transparentes ou a troco de contrapartidas. Por exemplo, a troco de descontos ou outras ofertas comerciais ou até mesmo como condição do acesso a um serviço.

Por outro lado, continuam a existir vários equívocos na utilização do fundamento «interesse legítimo», que se encontra sujeito a um teste individual de equilíbrio. Ou seja, tem de haver um equilíbrio entre os interesses do responsável pelo tratamento e dos titulares dos dados.

Este teste deve ser realizado por cada responsável que pretenda utilizar esse fundamento e requer uma avaliação cuidada, que nem sempre está a ser realizada, tendo em conta (i) o objetivo pretendido, (ii) a necessidade e (iii) o equilíbrio, e que tem de ser feita antes da operação de tratamento.

Se, a partir deste teste, se concluir que (i) a utilização dos dados não é razoável; (ii) os titulares dos dados já não esperariam um tratamento adicional; ou (iii) o tratamento causa danos injustificados, o fundamento «interesse legítimo» não pode ser utilizado. Em contraposição, há situações em que o interesse legítimo pode ser justificado, por exemplo, em situações de marketing, quando estejam em causa produtos e serviços semelhantes a outros já adquiridos e desde que seja assegurado o direito de, a todo o tempo, deixar de receber comunicações («opt-out»), ou quando responsáveis pelo tratamento de um grupo empresarial pretendam transmitir dados no âmbito do grupo de empresas para fins administrativos.

DIREITOS DE INFORMAÇÃO, ACESSO E PORTABILIDADE AINDA POR ASSEGURAR

O exercício dos direitos dos titulares dos dados não está a ser assegurado de forma cabal. As empresas são obrigadas a prestar informações de uma forma concisa, transparente, inteligível e facilmente acessível, o que nem sempre acontece.

Na elaboraçao das políticas de privacidade é de evitar a utilização de linguagem jurídica ou muito complexa. O texto deve ser o mais acessível e conciso possível, mas sem deixar de incluir todas as informações relevantes que são reccomendadas pelo CEPD, incluindo, o que, na maioria dos casos não tem ocorrido, uma lista das entidades com as quais a empresa partilha os dados.

Por outro lado, quando esteja em causa o tratamento de dados de crianças, a obrigação de prestação de informações, de forma simples e acessível, deve ser ainda mais rigorosa, sob pena de violação do dever de informação.

O exercício de direito de acesso aos dados pessoais encontra ainda vários entraves, havendo uma falta generalizada de mecanismos de acesso eficazes.

A iliteracia digital tão-pouco ajuda ao exercício de direitos pelos utilizadores, que desconhecem os direitos que lhes assistem e sem consciência que dados inferidos, por exemplo, através de visitas a sítios de Internet, da utilização de cookies intrusivos que permitam a geolocalização ou a definição de perfis de comportamento, são também dados pessoais.

O exercício dos direitos dos titulares dos dados deve ser facilitado, em particular o direito de acesso quando estejam em causa tratamentos de dados automatizados, incluindo definição de perfis. As plataformas de Internet têm, todavia, colocado entraves em divulgar perfis de comportamento de utilizadores. Espera-se, no entanto, que o Digital Services Act e o Digital Market Act, ainda em fase de proposta, possam vir a contribuir para alterar a atual realidade.

Também existem reservas quanto à portabilidade dos dados com a criação de entraves à transmissão dos dados de uma entidade para outra, bem como à anonimização dos dados, em cumprimento dos princípios da minimização dos dados e da limitação da finalidade, mecanismo eficaz para previnir a divulgação não autorizada, a usurpação de identidade e outras formas de utilização abusiva dos dados pessoais.

PROTEÇÃO DESDE A CONCEÇÃO E POR DEFEITO E AVALIAÇÃO DE IMPACTO

A proteção de dados desde a conceção e por defeito visa assegurar as medidas técnicas e operacionais necessárias para a aplicação dos princípios da minimização dos dados, limitação da finalidade e proteção dos direitos dos titulares dos dados.

A adoção destas medidas deve ser acompanhada por uma clara definição do papel dos fabricantes de tecnlogias de informação, ou seja, se atuam como responsáveis pelo tratamento ou subcontrantes. Estes conceitos (de responsável pelo tratamento e subcontratante) são concretizados nas Orientações 07/2020 do CEPD de 2 de setembro de 2020.

A proteção de dados desde a conceção e por defeito pressupõe ainda uma supervisão pelas autoridades de controlo quanto a uma correta utilização de configurações predefinidas pelos principais prestadores de serviços em linha, que estão obrigados a assegurar que, por defeito, só são tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, bem como que o titular dos dados pode exercer o seu direito de oposição por meios automatizados, quando esteja em causa a utilização de serviços da sociedade da informação.

Em outubro de 2020, o CEPD adotou as Orientações 04/2019 relativas à proteção de dados desde a conceção e por defeito.

Sempre que o tratamento dos dados seja suscetível de resultar num elevado risco para os direitos e as liberdades dos indivíduos, é necessário a realizar uma avaliação de impacto sobre a proteção de dados (AIPD). Um elenco (não taxativo) de operações de tratamento sujeitas a AIPD encontra-se previsto no Regulamento n.º 1/2018 da CNPD. De entre as quais: criação de perfis em grande escala; rastreamento da localização ou de comportamentos; tratamento de dados biométricos para identificação inequívoca de crianças ou trabalhadores; tratamento de categorias especiais de dados ou de dados altamente pessoais com recurso a novas tecnologias.

Uma AIPD pressupõe uma avaliação dos riscos para os direitos e liberdades dos indivíduos e identificar as medidas para fazer face aos riscos. Se a partir da AIPD se concluir que o tratamento resultaria num elevado risco na ausência de medidas, será necessário proceder a uma consulta prévia à CNPD. Até à data, foram seis as deliberações da CNPD emitidas na sequência de consulta prévia – uma em 2019 e cinco em 2020 –, entre as quais a relativa ao uso da aplicação "StayAway Covid" (Deliberação 277/2020).

TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

O acórdão «Schrems II» considerou inválido, com efeitos imediatos, o Estudo de Privacidade. Os operadores económicos terão, assim, de lidar com várias as questões quando transfiram dados da UE para os Estados Unidos.

Em julho de 2020, o Tribunal de Justiça da EU (TJUE) considerou que o Escudo de Privacidade, ao permitir intromissões desproporcionais nos direitos fundamentais dos indivíduos, nomeadamente por agências de segurança norte-americanas, como o FBI e a NSA, não assegurava uma proteção adequada dos dados. Em questão estava o acesso a dados pessoais transferidos para a sede do Facebook Inc., na Califórnia, através do Facebook Ireland, pelas autoridades públicas dos Estados Unidos.

No mesmo acórdão, o TJUE pronunciou-se sobre a validade das cláusulas contratuais-tipo, uma das soluções alternativas ao Escudo de Privacidade. O TJUE considera que as cláusulas-contratuais tipo são válidas, mas que a sua utilização, por si só, não assegura a licitude das transferências internacionais de dados. O que vale não apenas para as transferências para os Estados Unidos mas para países terceiros em geral.

A possibilidade de transferir dados pessoais com base em cláusulas contratuais-tipo (um novo projeto de cláusulas contratuais-tipo foi publicado pela Comissão Europeia em 12 de novembro de 2020) ou em regras vinculativas aplicáveis às empresas fica dependente do resultado da avaliação da legislação dos países terceiros. É necessário verificar se é assegurado um nível de proteção equivalente ao concedido na UE ou se é necessário implementar medidas adicionais. Em 10 de novembro de 2020, o CEPD emitiu dois conjuntos de recomendações: (i) um relativo às medidas adicionais (Recomendações 01/2020), que inclui seis passos, bem como exemplos de medidas adicionais, entre as quais, a reavaliação do nível de proteção e a monitorização; e (ii) outro relativo às Garantias Europeias Essenciais (Recomendações 02/2020). Outra solução é o recurso às derrogações previstas no artigo 49.º do RGPD, em particular o consentimento. Trata-se, no entanto, de uma solução que deverá restringir-se a situações específicas.

São várias as questões a considerar nas transferências de dados e que não se limitam à adoção de uma das soluções ou combinação de soluções do RGPD, mas que antes pressupõem a adoção de salvaguardas adicionais no sentido de verificar se o país terceiro assegura um nível de proteção equivalente ao da UE.

IMPLEMENTAÇÃO DO RGPD A DIFERENTES VELOCIDADES

O RGPD visa a harmonização das regras de proteção de dados na UE. É, todavia, ainda distinta a sua implementação, variando o grau de maturidade de país para país. Em cada país, as PMEs não evoluíram ao mesmo ritmo das grandes empresas.

A implementação do RGPD não tem sido igual em todos os Estados-membros, variando o nível, grau de maturidade, inclusive das autoridades de controlo (em termos de orientações, prática decisória), e as sanções.

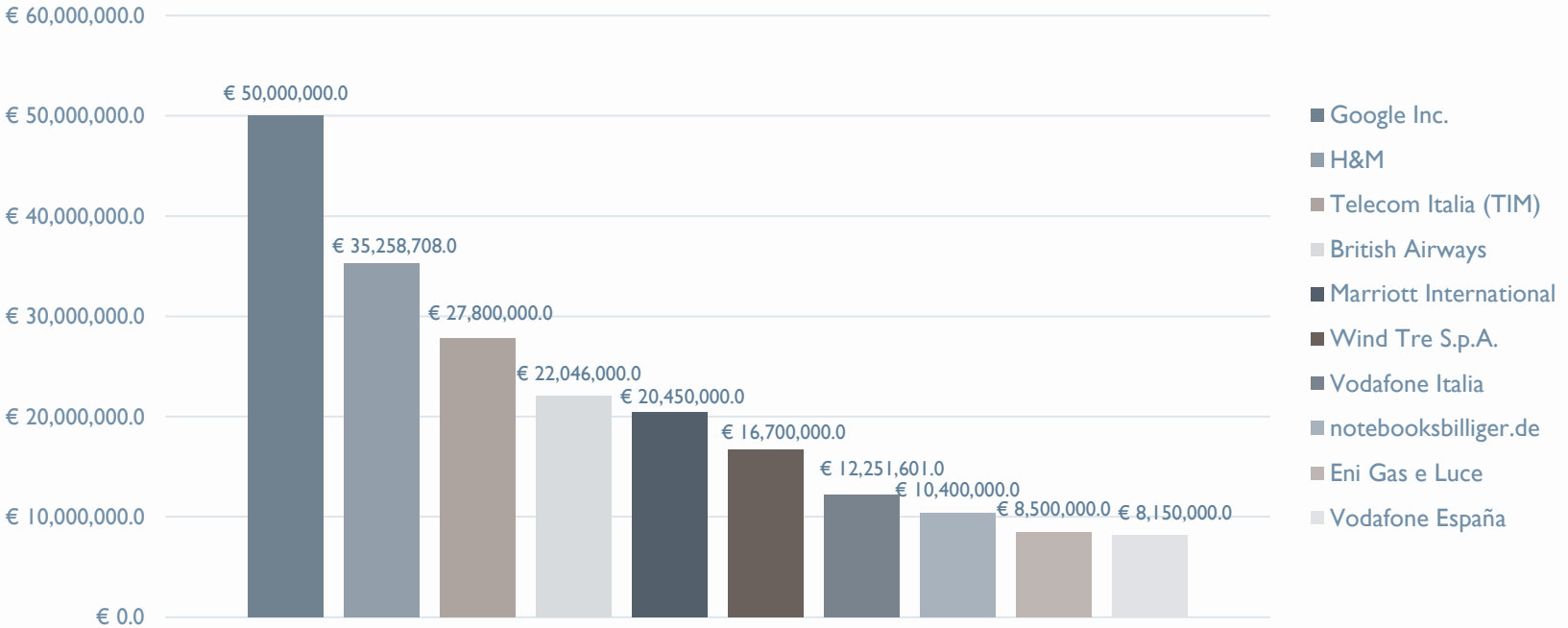
As cinco maiores coimas foram aplicadas pelas autoridades de controlo francesa (à Google Inc.), inglesa (à British Airways e à cadeia de hotéis Marriott International), alemã (à retalhista H&M) e italiana (à Telecom Italia – TIM, operadora de telecomunicações). Estas cinco coimas perfazem o montante total de cerca € 155 milhões, já contando com a significativa redução do montante das coimas de que beneficiou a British Airways e a Marriott International, devido a quebras significativas na sua atividade por força da pandemia. A ordem das centenas de milhões de euros acabaria, assim, por ser reduzidas para as dezenas de milhões pela autoridade inglesa no atual contexto de pandemia

A falta de fundamento de licitude do tratamento de dados foi a principal violação que motivou as coimas aplicadas, seguindo-se da falta de adoção das medidas técnicas e organizativas adequadas à segurança do tratamento.

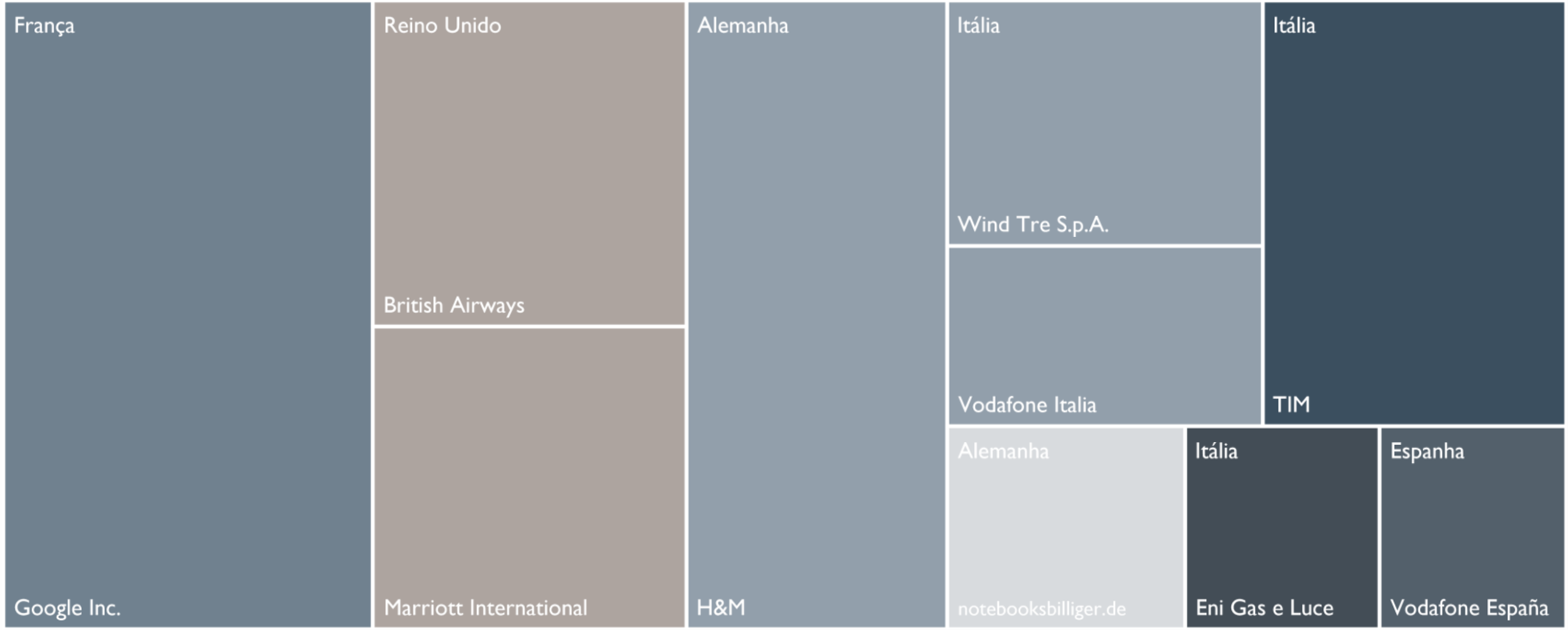
Apesar de o RGPD conferir alguma margem de flexibilidade às empresas quanto à escolha dos fundamentos de licitude dos seis possíveis (por exemplo, consentimento ou interesse legítimo; consentimento ou execução de um contrato) ou quanto às medidas de segurança a adotar, é necessário fazer uma escolha consciente e ponderar o seu impacto para o dia-a-dia da empresa, assim como ter um plano de resposta bem definido em caso de violação de dados pessoais. Se para uma organização de grande dimensão, com mais recursos financeiros e humanos (inclusive um Encarregado de Proteção de Dados), esta tarefa poderá revelar-se mais fácil, para as pequenas e médias empresas nem sempre será assim,

Por outro lado, há setores de atividade/indústrias mais propícias a escrutínio, nomeadamente, as que tratam um elevado volume de dados pessoais, como é o caso das telecomunicações, das plataformas digitais, o que explica, assim, que, de entre as dez maiores coimas aplicadas, uma delas tenha sido à Google e a quatro operadores de telecomunicações, Telecom Italia, Wind Tre, Vodafone Italia (três operadoras italianas) e à Vodafone España.

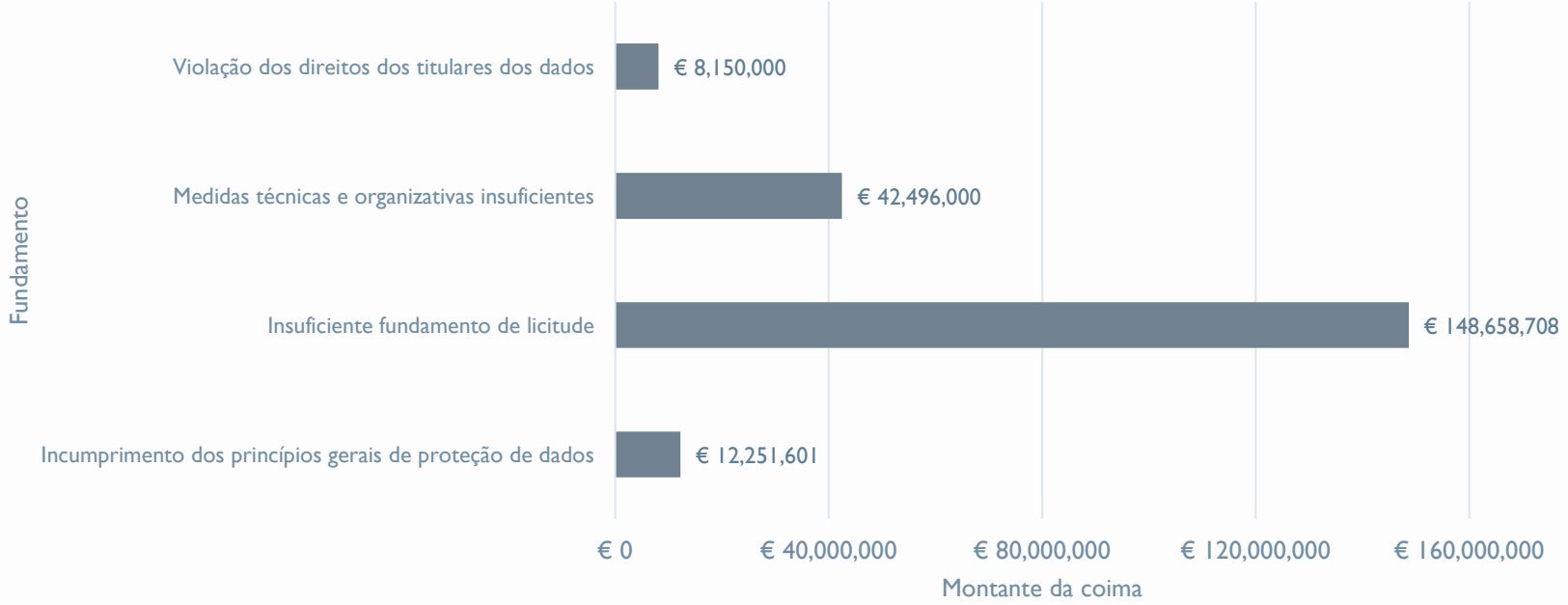
AS 10 MAIORES COIMAS NA UE (2018-2021)



AS 10 MAIORES COIMAS NA UE (2018-2021)



AS 10 MAIORES COIMAS NA UE (2018-2021)



PONTO DA SITUAÇÃO EM PORTUGAL

Em Portugal, a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade nacional de controlo. Nestes três últimos anos, a CNPD tem-se deparado com vários desafios, entre os quais:

- A tardia aprovação, mais de um ano depois da data de aplicação do RGPD, da lei nacional de execução – a Lei n.º 58/2019, de 8 de agosto – e que alterou e republicou a lei de organização e funcionamento da CNPD, conferindo-lhe personalidade jurídica e autonomia administrativa e financeira, para garantir o regime de independência da CNPD;
- Críticas a algumas normas da Lei n.º 58/2019, por considerar que contradizem o RGPD ao abrigo do princípio do primado do Direito da UE e que levaram a CNPD a emitir duas deliberações sobre a necessidade de desaplicação futura de algumas das normas da Lei n.º 58/2019 (Deliberação/2019/494) e a interpretação que faz do artigo 44.º, n.º 2, da Lei n.º 58/2019, quanto à dispensa de aplicação de coimas às entidades públicas (Deliberação/2019/495);
- A falta de recursos humanos e de meios técnicos para assegurar o exercício cabal das suas competências de orientação prévia, fiscalização e de correção dos tratamentos dos dados; e
- O contexto pandémico com um aumento exponencial de tratamentos de dados pessoais nas áreas da saúde, laboral e do ensino, em muitos casos sem enquadramento legal direto e com impacto significativo no dia-a-dia dos cidadãos, e que exigiu um acompanhamento e análise contínuos pela CNPD.

Em 2020, a CNPD aprovou sete orientações, em particular, sobre a recolha de dados de saúde dos trabalhadores, utilização de tecnologias de suporte do ensino à distância, medição da temperatura corporal.

No âmbito da averiguação e de avaliação de impacto de proteção de dados, a CNPD emitiu três deliberações relativas (i) à averiguação efetuada pela CNPD sobre o funcionamento da plataforma Trace Covid-19; (ii) à consulta prévia relativa à avaliação de impacto sobre a proteção de dados quanto a um sistema para identificação da taxa de ocupação das praias (Smart Crowd); e (iii) à consulta prévia relativa à avaliação de impacto sobre a proteção de dados quanto ao sistema de rastreio de contactos de proximidade para dispositivos móveis digitais, denominado STAYAWAY COVID.

AS COIMAS APLICADAS PELA COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

Em 2018, a CNPD aplicou uma coima, no valor de € 400.000, ao Centro Hospital Barreiro-Montijo, deixando claro que as entidades públicas não ficariam a coberto de uma dispensa de aplicação de coimas ao abrigo do RGPD, embora a prática da infração em causa tivesse sido anterior à aplicação do RGPD.

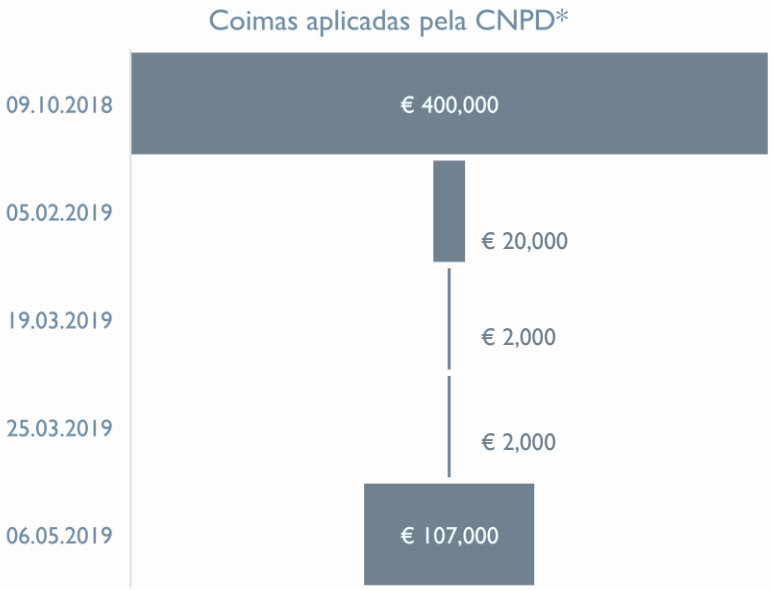
De acordo com o Relatório de Atividades da CNPD de 2019/2020, publicado em 30 de março de 2021, a CNPD aplicou um total de 34 coimas em 2019, num montante de cerca de € 600,000. Entre estas sanções pecuniárias, sete corresponderam a infrações ao RGPD, no valor de € 410,000, tendo as restantes sido aplicadas ao abrigo da anterior lei de proteção de dados (Lei n.º 67/98, de 26 de outubro), por ser o regime mais favorável em processos anteriores à aplicação do RGPD, bem como ao abrigo da legislação sobre a privacidade nas comunicações eletrónicas (Lei n.º 41/2004, de 18 de agosto).

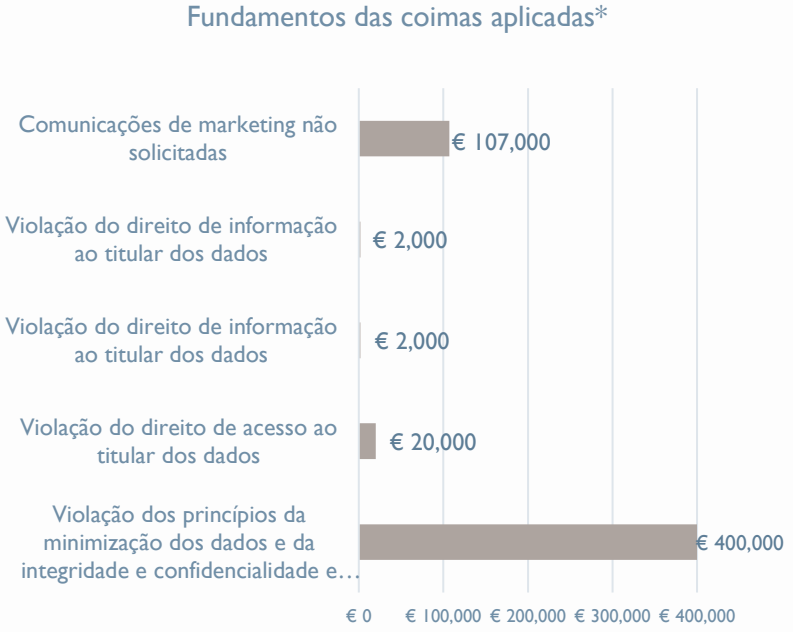
Das deliberações publicadas no sítio de Internet da CNPD (www.cnpd.pt), é possível constatar que, em 2019, houve quatro coimas nos montantes de € 20,000, € 2,000, € 2,000 e € 107,000, que foram aplicadas a entidades cuja identidade não se conhece, uma vez que a CNPD não publica a identidade das entidades sujeitas a coima.

De entre essas quatro coimas, a mais elevada, de €107,000, deveu-se a comunicações de marketing não solicitadas. As restantes três, a violações dos direitos de acesso e informação dos titulares dos dados.

No ano de 2020, o mesmo Relatório de Atividades refere que a CNPD aplicou 15 coimas, no valor de € 47,000, a maior das quais ao abrigo da legislação sobre a privacidade nas comunicações eletrónicas, por envio de marketing em violação das regras legais (spam). Fazendo uma pesquisa pelas deliberações publicadas em 2020 no sítio de Internet da CNPD, não encontrámos, todavia, essas deliberações. Com base nas deliberações publicadas no sítio de Internet, a CNPD aplicou as seguintes coimas:

AS COIMAS APLICADAS PELA CNPD





**De acordo com as deliberações publicadas no sítio de Internet da CNPD.*

PRÓXIMOS DESAFIOS

Ao longo dos últimos anos, as tecnologias digitais têm vindo a transformar a economia e a sociedade, afetando todos os setores de atividade e o dia-a-dia dos cidadãos à escala mundial. Os dados em geral e os dados pessoais em particular estão no centro desta transformação, que tem sido acompanhada por vários desafios, sobretudo no contexto de uma economia digital.

Adensa-se, por isso, a necessidade de uma rigorosa aplicação do RGPD e a sua inevitável articulação com legislação em domínios como os da publicidade em linha, do microdirecionamento e da definição algorítmica de perfis, da classificação, disseminação e amplificação de conteúdos pelas plataformas digitais, e o da cibersegurança.

O RGPD, que oferece as "linhas mestras" para a proteção dos dados pessoais e privacidade, não está (e não deve estar) isolado, como, alias, demonstram as recentes iniciativas legislativas da UE que, de uma forma ou outra, têm impactos na proteção de dados. Disso são exemplos as propostas de Regulamento de Governação de Dados, dos Serviços Digitais (*Digital Services Act*) e do Mercado Digital (*Digital Market Act*), do regulamento relativo à privacidade nas comunicações eletrónicas (*e-privacy*), do regulamento sobre a abordagem europeia para a inteligência artificial.

Um dos próximos desafios para a proteção de dados será o da articulação entre as diferentes iniciativas legislativas e o de conseguir alcançar a desejável coerência, que não será fácil com tantos interesses em jogo – o dos "utilizadores digitais" (consumidores), das plataformas digitais com diferentes dimensões e independências entre si, das empresas de marketing e publicidade e do mercado em geral – e a criação de entraves a uma sã concorrência.

A articulação entre o regime da proteção de dados e a defesa da concorrência será outro dos desafios, com a necessidade de adaptação das regras de concorrência à economia digital, em particular em matéria de acordos restritivos/práticas concertadas e abusos de posição dominante.

A curtíssimo e curto prazos, há também desafios a considerar, como o do certificado digital da Covid-19, o das transferências internacionais de dados, quanto ao Brexit e às transferências de dados para os EUA. Quanto a estas últimas, impõe-se uma rápida e fazível solução.

Estamos na "era dos dados", pelo que velhos e novos desafios serão, de certo, uma constante e o difícil será mesmo a legislação de proteção de dados conseguir acompanhar o ritmo do desenvolvimento tecnológico.

MACEDO▪VITORINO

SOBRE A MACEDO VITORINO

&

MVCOMPLIANCE

QUEM SOMOS

A MACEDO VITORINO foi fundada em 1996, centrando a sua atividade na assessoria a clientes nacionais e estrangeiros em sectores específicos de atividade, de que destacamos o sector financeiro, as telecomunicações, a energia e as infraestruturas.

Desde a sua constituição, a MACEDO VITORINO estabeleceu relações estreitas de correspondência e de parceria com algumas das mais prestigiadas sociedades de advogados internacionais da Europa e dos Estados Unidos, o que nos permite prestar aconselhamento em operações internacionais de forma eficaz.

As nossa atuação é citada pelos diretórios internacionais, Legal 500, IFLR 1000 e Chambers and Partners, nomeadamente nas áreas de Direito Bancário & Financeiro, Societário e «M&A», Mercado de Capitais, Direito Fiscal, Projetos e Contencioso.

Em janeiro de 2021, a MACEDO VITORINO lançou o programa **MV**COMPLIANCE, para assessorar as empresas em diversas matérias de «compliance», porque o «compliance» deve estar no topo das prioridades das empresas, sob pena de ficarem sujeitas a pesadas multas e danos à sua reputação junto de colaboradores, clientes, e da sociedade em geral.

Criámos uma equipa multidisciplinar dedicada a:

- GOVERNO SOCIETÁRIO
- BRANQUEAMENTO DE CAPITAIS
- RESPONSABILIDADE SOCIAL E LABORAL
- PRIVACIDADE E PROTEÇÃO DE DADOS
- CONCORRÊNCIA
- RESPONSABILIDADE AMBIENTAL

MACEDO▪▪VITORINO

CONTACTOS:
CLÁUDIA FERNANDES MARTINS
CMARTINS@MACEDOVITORINO.COM

TEL. (351) 213 241 900
RUA DO ALECRIM, 26E 1200-018 LISBOA
PORTUGAL
MACEDOVITORINO.COM