MACEDO VITORINO

BREVES NOTAS SOBRE O ATUAL PONTO DA SITUAÇÃO E DESAFIOS

RGPD, QUATRO 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 quatro anos, que acrescem aos dois anos de vigência do RGPD e de (suposta) 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.

Os últimos anos foram anos *sui generis*, marcados 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 significativo 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 alguns dos 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 usar 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 usar 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 é 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 recomendadas pelo CEPD, incluindo, o que, na maioria dos casos não ocorre, 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.

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 "StayAwayCovid" (Deliberação 277/2020).

TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

A Comissão Europeia e os Estados Unidos anunciaram terem chegado a um acordo preliminar para as transferências de dados pessoais entre a União Europeia e os Estados Unidos.

Na sequência de o Tribunal de Justiça da UE (TJUE) ter considerado inválidos os dois anteriores acordos estabelecidos entre a União Europeia e os Estados Unidos da América – o "*Safe Harbor*", em 2015, e o "*Privacy Shield*" em 2020 –, os EUA e a UE anunciaram um acordo preliminar para as transferências de dados e que terá em consideração as preocupações levantadas pelo TJUE.

Em julho de 2020, o 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 considerou que as cláusulas-contratuais tipo são válidas, mas que a sua utilização, por si só, não asseguraria a licitude das transferências internacionais de dados. O que vale não apenas para as transferências para os Estados Unidos, mas para os países terceiros em geral.

Com este acordo preliminar, os EUA assumiram uma posição sem precedentes, ao introduzir reformas para reforçar a proteção da privacidade e as liberdades civis "aplicáveis a atividades de inteligência de sinais" ("Signal Intelligence Collection"), nomeadamente recolha de e-mails, mensagens de texto e outras comunicações eletrónicas por agências de inteligência.

Para os cidadãos e empresas, este acordo irá trazer claros benefícios, nomeadamente ao constituir uma solução jurídica fiável e duradoura para as transferências de dados entre a UE e os EUA, as quais representam anualmente mais de $1 trilião de Dólares para o comércio transfronteiriço, promovendo uma economia digital mais competitiva e uma forte cooperação económica entre ambos os lados do Atlântico.

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 organizações também não evoluem ao mesmo ritmo.

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 luxemburguesa (à AmazonEurope S.a.r.l.), irlandesa (ao Whatsapp) e francesa (à Google LLC, ao Facebook Ireland Ltd. e à Google Ireland Ltd.).

Estas cinco coimas perfazem o montante total de cerca € 1,1 mil milhões.

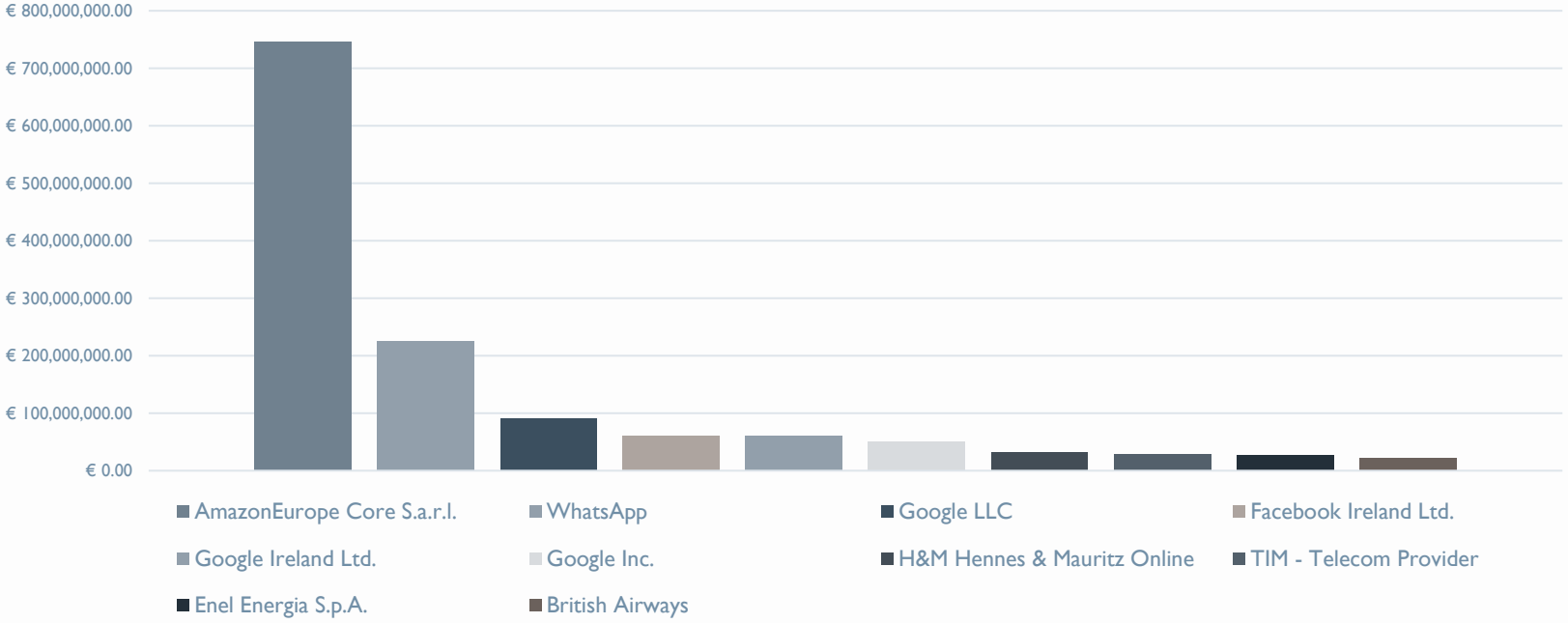
A falta de fundamento de licitude do tratamento de dados foi a principal violação que motivou as coimas aplicadas, seguindo-se da falta de adoção das medidas técnicas e organizativas adequadas à segurança do tratamento.

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.

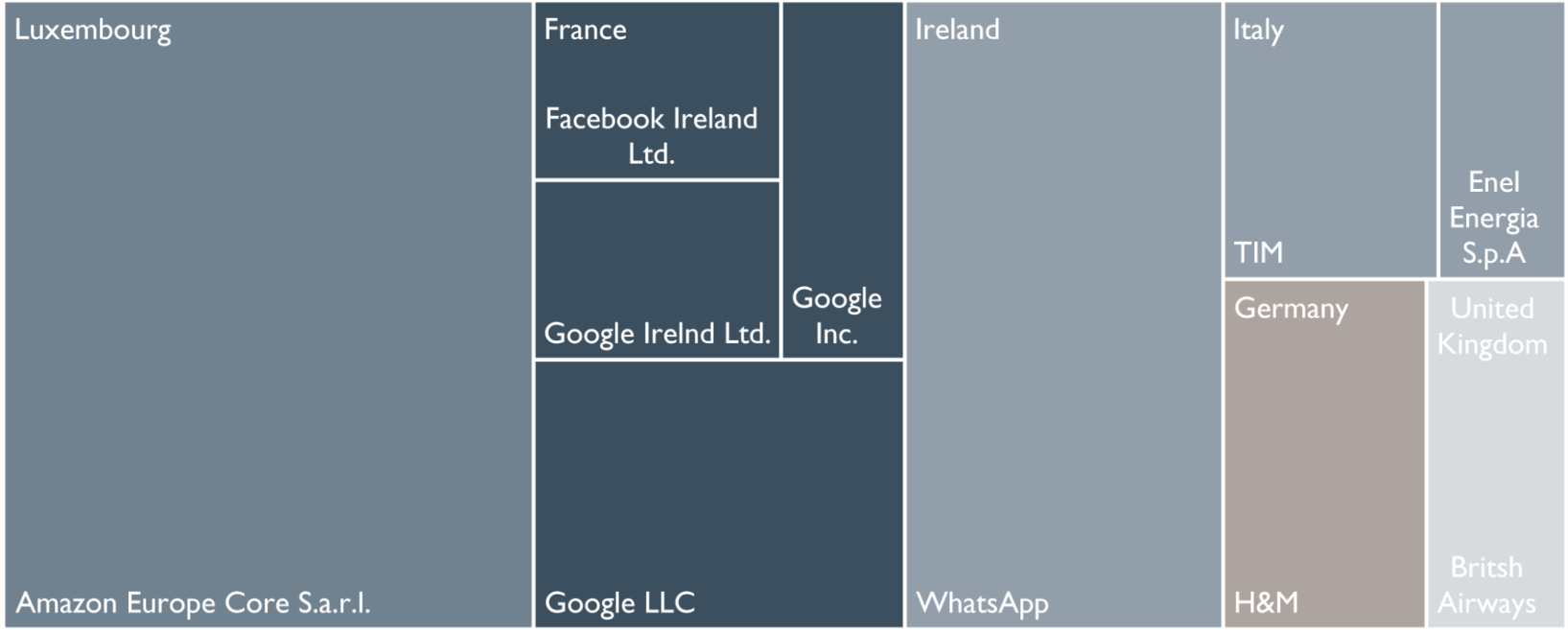
Se para uma organização de grande dimensão, com mais recursos financeiros e humanos (inclusive um Encarregado de Proteção de Dados), esta tarefa poderá revelar-se mais fácil, para as pequenas e médias empresas nem sempre será assim,

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 e das plataformas digitais, o que explica, assim, que, de entre as dez maiores coimas aplicadas, três delas dizem respeito a plataformas digitais e uma delas à Telecom Italia.

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 quatro 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 não aplicação 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, e emitiu três deliberações no âmbito da averiguação e de avaliação de impacto de proteção de dados, em particular quanto à aplicação de rastreio STAYAWAY COVID.

Estes números contrastam com os de 2021. Da informação disponível no sítio de Internet da CNPD não constam orientações e deliberações no âmbito da averiguação e de avaliação de impacto no último ano.

A CNPD emitiu, todavia, um regulamento relativo aos requisitos adicionais de acreditação para os organismos de certificação – o Regulamento n.º 834/2021 –, bem como uma diretriz sobre comunicações eletrónicas de marketing direto dado o número crescente de participações de cidadãos relacionadas com comunicações eletrónicas não solicitadas para fins de marketing direto – a Diretriz/2022/1.

COIMAS APLICADAS PELA CNPD (2018-2021)

De acordo com dados recentemente divulgados pela CNPD, os processos de averiguações, violações de dados e coimas atingiram números máximos no quarto ano de aplicação do RGPD.

Em 2021, a autoridade de controlo registou um total de 318 notificações de violação de dados pessoais. De entre essas notificações, 250 foram no setor privado e 68 no setor público. No setor privado, a maior prevalência ocorreu na área de comércio e serviços (78 notificações), seguida da banca e seguros (42); e no setor público, relevaram os incidentes na administração local (27) e no ensino superior (24).

O maior aumento ocorreu, todavia, no âmbito da aplicação de coimas.

Em 2021, a CNPD aplicou 60 coimas, que representaram um valor total de 1,49 milhões de euros, o que incluiu sanções aplicadas ao abrigo do RGPD e da lei da privacidade nas comunicações eletrónicas, nomeadamente por violação das regras relativas a publicidade não solicitada e gravações de chamadas telefónicas.

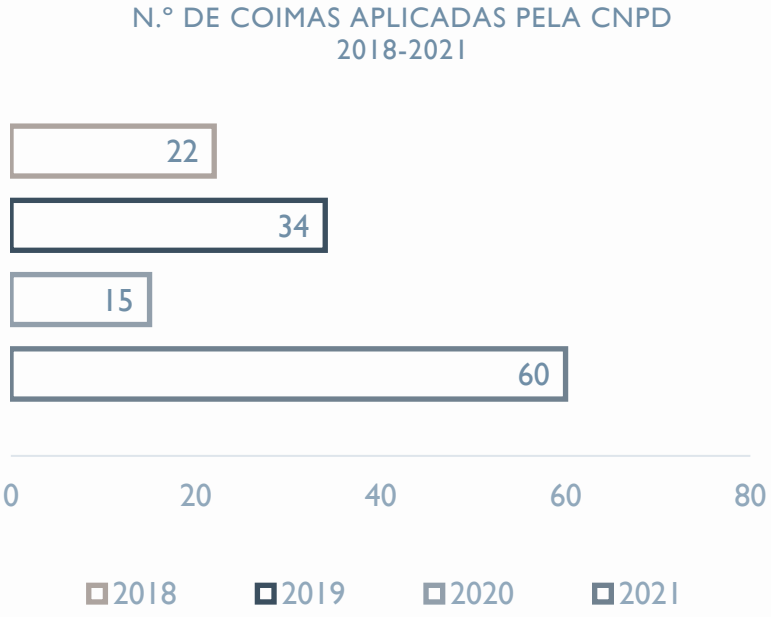
Este valor contrasta com as 15 coimas aplicadas em 2020, no valor de 47 mil euros, e as 34 de 2019, num valor de cerca de 600 mil euros, sendo que apenas sete destas sanções foram infrações ao RGPD (410 mil euros) e as restantes foram aplicadas ao abrigo da anterior legislação. No ano de 2018 a contar da data de aplicação do RGPD, a CNPD aplicou 22 coimas, que ascenderam a 408 mil euros.

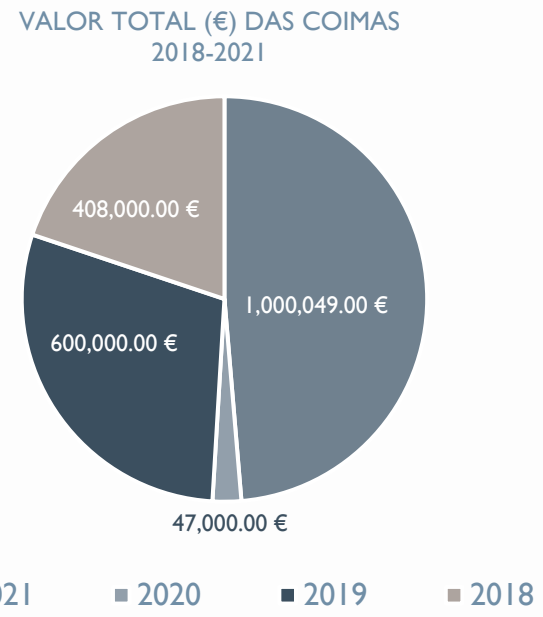
Desde 25 de maio de 2018, as coimas aplicadas pela CNPD representam um total de 131 coimas, que originaram mais de 2,54 milhões de euros.

Nos primeiros meses de aplicação do RGPD, a CNPD aplicou logo 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 forma coerente, o ano que passou ficou marcado por mais uma coima exemplar a uma entidade pública. Em janeiro de 2022, a CNPD aplicou uma coima no valor de 1,25 milhões de euros ao Município de Lisboa por envio de dados de ativistas às autoridades russas. Fazendo lembrar, mais uma vez, que nenhuma entidade se encontra "a salvo" da não aplicação do RGPD.

COIMAS APLICADAS PELA CNPD (2018-2021)





PRÓXIMOS DESAFIOS – EM GERAL

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.

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.

PRÓXIMOS DESAFIOS – NO CONTEXTO NACIONAL

A implementação do RGPD não é uma tarefa fácil e deve ser transversal a todas as organizações, não podendo ficar-se pela publicação de um conjunto de políticas e códigos e meras alterações formais, sem qualquer adesão ao contexto organizacional e envolvimento dos colaboradores.

Em qualquer circunstância, a implementação do RGPD nunca poderá ser resolvida por uma só pessoa – o *Data Protection Officer* (**DPO**) –, sem a participação ativa e proativa dos demais colaboradores e sem que a organização esteja ciente ou preparada para alterar padrões de comportamento, a sua cultura organizacional.

A função de DPO é difícil e exigente. Os DPOs têm de ter experiência, têm de ter formação, têm de se atualizar permanentemente, têm de ter ajuda externa, têm de ter a colaboração, o respeito e a ajuda dos demais colaboradores da organização.

Em muitos casos, a função de DPO é desempenhada por colaboradores da própria organização, que acumulam essa função com outras funções que já desempenhavam originalmente e que por uma questão de necessidade e de poupança de recursos se veem obrigados a aceitar.

Por contraposição, o papel dos restantes colaboradores é, não raras vezes, insuficiente ou quase inexistente em matéria de proteção de dados, correndo a organização o sério risco de acabar por falhar e, desta forma, todos falham.

Está em causa, sobretudo, um questão de falta de "cultura" das organizações. Ou seja, muitas organizações públicas e privadas habituaram-se a fazer o que sempre foi feito, porque sempre foi feito assim, o que lhes dá uma ilusão de segurança, que é, na verdade, uma falsa segurança. O facto de ter sido sempre assim, feito pelas mesmas pessoas ou por outras que as antecederam na função, acabando por se transformar num processo mecânico, sem qualquer espírito crítico (ou autocrítico), não está bem e acaba por contaminar a organização e uma cultura de impunidade.

As questões associadas à proteção de dados pessoais (que sempre existiram, mas para as quais as pessoas não estavam alerta ou não lhes davam a devida importância) são propícias a encaixar-se nesse padrão de comportamento ainda recorrente nas organizações nacionais, sem nunca fazerem uma avaliação independente ou sequer uma autoavaliação, e sujeitando-se, assim, a pesadas sanções (não apenas financeiras, mas também reputacionais), que poderiam ser, à partida, evitadas.

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