DPO mag

EDIÇÃO Nº 9
JUL / 24

APDPO PORTUGAL

www.dpo-portugal.pt

DPO mag

EDIÇÃO Nº 9
JUL / 24

www.dpo-portugal.pt

DPO | magazine

FICHA TÉCNICA

NOME
DPO | magazine

PROPRIEDADE
APDPO Portugal – NIF 541502835

DIRETORA
Inês Oliveira

EDITOR
Luís Ferreira Mendes

PERIODICIDADE
Semestral

PREÇO
Gratuito

CONTACTO GERAL
geral@dpo-portugal.pt

UM PROJETO APDPO
ISSN 2184-8211

COPYRIGHT

DPO|magazine: a primeira revista do setor na Europa lançada a 28 de outubro de 2020.

ESTATUTO EDITORIAL

A DPO|magazine é um projeto de informação internacional que visa preencher espaços vazios e acrescentar valor ao campo da proteção e segurança dos dados e da informação.
A DPO|magazine tem carácter digital, é independente e livre, sem interesses partidários ou económicos, e sem estabelecer hierarquias de funções ou de sectores de atividade, nas suas opções editoriais.
A DPO|magazine pauta-se por padrões de exigência na qualidade da informação e do conhecimento que veicula, primeiro garante da sua credibilidade e afirmação.
A DPO|magazine não fixa fronteiras geográficas, culturais ou temporais, recusando situações de sensacionalismo, exploração ou especulação.
A DPO|magazine fomenta o debate consciente e respeitável das grandes questões que se colocam às sociedades atuais, na perspetiva da melhoria do conhecimento.
A DPO|magazine é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e disponibilidade quotidianas para o estímulo à reflexão e ao conhecimento.

CONTEÚDO

O Conteúdo da DPO|magazine estará em permanente adaptação, procurando satisfazer a necessidade de melhor exposição dos temas que elegemos para entregar aos nossos leitores.

Presentemente a revista organiza-se em:

| Artigos
| Conteúdos de parceiros
| Debates
| Entrevistas
| Informações institucionais
| Opiniões
| Publicidade
| Reportagens

A QUEM SE DESTINA?

| Administradores e Gestores de Empresas
| Cargos dirigentes da Administração Pública
| Encarregados de Proteção de Dados
| Técnicos de Proteção de Dados
| Técnicos de Compliance
| Advogados, Solicitadores e Agentes de Execução
| Consultores e Auditores
| Economistas e Contabilistas
| Engenheiros informáticos e de Arquitetura de Sistemas | Especialistas em Proteção e Segurança de Dados
| Especialistas em Segurança Informática e Cibersegurança | Especialistas em Sistemas de Informação
| Especialistas em Transformação Digital
| Gestores e Analistas de Dados
| Profissionais BAD, da Informação e do Conhecimento
| Técnicos de Informação e Comunicação
| Técnicos de Recursos Humanos

PUBLICIDADE

Dispomos das seguintes opções para inserção de anúncios: | 2 páginas
| 1 página
| 1/2 página horizontal


PORTUGAL

Mensagem da Diretora

Inês Oliveira

Presidente da Direção da APDPO

Diretora da DPO Magazine

Bem-vindos à DPO Magazine n.º 9! 9 edições de um projeto associativo que a Direção da APDPO se orgulha de dirigir.

Nesta mensagem inicial, permitam-me sublinhar que no passado dia 25 de maio se comemorou o 6.º aniversário da entrada em aplicação do RGPD, sendo a ocasião oportuna para balanços e antevisões no que à proteção de dados respeita.

Primeiro, quanto ao balanço de 6 anos de RGPD: o caminho da conformidade continua a ser difícil no dia a dia.

Por um lado, ainda enfrentamos muitos mitos, desconhecimento e falta de sensibilização para o tema, que diariamente todos os profissionais de proteção de dados tentam combater.

Por outro lado, nas organizações com um nível de maturidade face ao RGPD mais significativo, o trabalho no terreno visa dar resposta às oportunidades de crescimento da empresa/entidade sempre com foco na proteção das pessoas visadas, os titulares dos dados.

No desenvolvimento de um novo website ou app, na criação de um assistente virtual, na aquisição de um sistema aplicacional, na utilização de uma nova ferramenta de produtividade, por exemplo, a *check list* de conformidade RGPD tem de ser acautelada, sendo necessário avaliar:

- ✓ Licitude
- ✓ Transparência/fornecimento de informações ao titular dos dados
- ✓ Limitação das finalidades

- ✓ Tratamentos posteriores compatíveis e/ou conexos
- ✓ Minimização dos dados
- ✓ Exatidão
- ✓ Limitação da conservação
- ✓ Integridade e confidencialidade

Ainda sob outro prisma, de forma holística, a responsabilidade das organizações, que as obriga a evidenciar o cumprimento da legislação, é um princípio-regra que tem sido de difícil interiorização no seio das lideranças ao mais alto nível.

E tem sido difícil sobretudo porque a fiscalização e sancionamento não é visível nem sentido no terreno, o que faz com que as organizações esmoreçam a proteção de dados e se foquem nos outros – tantos – problemas diários.

Por fim, uma antevisão dos desafios no curto prazo.

Muitas organizações estão a debruçar-se sobre o impacto da inteligência artificial (IA) na sua atividade.

Pensemos no mais simples dos exemplos: um *chatbox* a disponibilizar que responde de forma particular e individualizada a um cliente/utente e cuja resposta se repercutirá em efeitos jurídicos na esfera da pessoa.

Estas caixas de conversação, suportadas em IA, que se diferenciam de um mero assistente virtual, porque não respondem de forma generalista, antes respondendo de forma direta e pessoal, colocam muitos desafios em sede de proteção de dados, mormente na sua fase primeira, a do treino.

De facto, as ferramentas que utilizam IA têm como fase necessária o treinamento, que na generalidade dos casos terá de ser feito com dados pessoais. E antes de todas as questões jurídicas, as organizações são levadas a ponderar todas as problemáticas éticas subjacentes, sendo este, pois, um dos grandes desafios que antevimos.

A Todos os profissionais de proteção de dados se exigirá rigor na interpretação da lei. E bom-senso!

Está lançada a nona edição da revista da APDPO. Cumpre-me agradecer, em nome da Associação, o empenho de Todos aqueles que contribuíram para mais esta edição.

Boas leituras e vemo-nos na próxima edição!

Conteúdo

JAVALI
OPEN SOURCE SYSTEMS

A solução web à medida do seu negócio

+ 20 anos experiência

+ 300 clientes satisfeitos

+ 10 setores de atividade

+ 300 projetos desenvolvidos

Serviços e soluções para projetos de sucesso

- Consultoria
- Gestão de Projeto
- Web Design
- Desenvolvimento web - Drupal
- Formação
- Suporte pós-produção
- Manutenção
- Websites
- Intranets
- Lojas online
- Plataformas para Instituições de Ensino
- Plataforma para Rent-a-Car
- Desenvolvimento à medida

MINISTÉRIO PÚBLICO
PORTUGAL

"Vimos por este meio expressar o gosto que tivemos em trabalhar com a Javali, foi extremamente gratificante, em grande parte pela sintonia e perfeita colaboração com a PGR, mas também, e sobretudo, pela extrema simpatia da vossa equipa, disponibilidade, profissionalismo e competência."

Nelson Coelho e Cândida Ferreira, Procuradoria-Geral da República

CASCAIS
Tudo começa nas pessoas

"Quando a Câmara Municipal de Cascais apostou na criação do seu novo portal, a Javali foi a empresa escolhida para a sua implementação. De lá para cá têm sido nossos parceiros na manutenção técnica e evolutiva do portal, dando resposta na íntegra às necessidades de um projeto que sabemos inovador e criativo."

Matilde Cardoso, Câmara Municipal de Cascais

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

BANCO DE PORTUGAL
EUROSISTEMA

Secretaria-Geral da Educação e Ciência

DGES
Direção-Geral do Ensino Superior

UCCLA

GRUPO Manuel Champalimaud

sumol+compal
É da nossa natureza.

omi

Ispa

NOVA
FACULDADE DE CIÊNCIAS E TECNOLOGIA

NICE RENT

Oliveira Seguros

esop

Contacte-nos

(+351) 212 957 215 | info@javali.pt | www.javali.pt

Transferência Internacional de Dados: os desafios corporativos

Andrezza Hautsch Oikawa

Sócia da Advocacia Correa de Castro;

DPO – Tudo Azul S.A.

Advocacia Correa de Castro; Tudo Azul S.A.

Em um cenário em que o compartilhamento de informações não encontra fronteiras físicas, as corporações enfrentam grandes desafios para realizar a transferência internacional de dados pessoais em conformidade com as normas que disciplinam o tratamento de dados pessoais, em especial o Regulamento Geral sobre Proteção de Dados ("RGPD"). Dentre esses desafios destaca-se a transferência para plataformas de serviços digitais, destacadamente as "Big Techs".

No ambiente corporativo, a contratação dos serviços das "Big Techs" para dar suporte às atividades cotidianas é necessária. Quantas são as empresas que contratam Google, Microsoft, Amazon, Apple, dentre outros, para serviços de *cloud*, correio eletrônico, aplicativo de mensagens? E, como não contratar? Sendo inevitável a contratação, considerando que a maioria das *Big Techs* está localizada fora do território europeu, como seguir de forma segura?

É fato que a utilização das plataformas digitais, via de regra, traz consigo a transferência internacional de dados pessoais. E, portanto, sujeita-se às regras comunitárias de proteção de dados pessoais

O RGPD, em seu artigo 44º, estabelece que a transferência internacional de dados para países terceiros deve respeitar o regulamento e seguir as condições estabelecidas nos artigos 45º

(Transferências com base em uma Decisão de Adequação) ou 46º (Garantias Adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes). Nesse contexto, responsáveis pelo tratamento e subcontratantes estão sujeitos a ditas regras.

De forma a atender o disposto no RGPD e transferir os dados de forma segura é importante que as empresas implementem um procedimento específico para essa finalidade.

Como um primeiro passo, recomenda-se a identificação de todas as atividades relacionadas aos serviços digitais a serem contratados, bem como os dados pessoais que serão tratados, os eventuais riscos e seus impactos aos direitos civis.

O próximo passo consiste em uma ampla análise da plataforma de serviços digitais, as garantias por ela fornecidas para o tratamento seguro dos dados pessoais e para que países haverá a transferência.

Então, deve-se verificar se o país para o qual os dados serão transferidos está sujeito a uma decisão de adequação pela Comissão. Em havendo uma decisão de adequação, cabe à empresa formalizar em contrato as condições convencionais para o tratamento de dados pessoais com a plataforma de serviços digitais.

Não existindo uma decisão de adequação, é fundamental que a contratação da plataforma de serviços digitais esteja respaldada em cláusulas-tipo de proteção de dados pessoais que tragam as garantias de tratamento dos dados pessoais sob os termos do RGPD.

No entanto, a possibilidade da utilização das cláusulas-tipo não obsta a necessidade de que o país para o qual os dados serão transferidos também apresente garantias de respeito à proteção de dados pessoais. Caso contrário, a transferência de dados, mesmo que ao abrigo de uma cláusula-tipo, poderá ser entendida ilegal.

Considerando que grande parte das *Big Techs* está localizada nos Estados Unidos, cujas leis de vigilância permitem que órgãos da administração pública, sem a devida transparência, acessem dados pessoais (incluindo dados de cidadãos europeus) tratados por empresas, como seguir?

Bem se sabe, que Estados Unidos e a União Europeia nos últimos 20 anos, negociaram três "acordos" para a transferência internacional de dados, sendo que os dois primeiros "Safe Harbor" e "Privacy Shield" foram considerados ilegais em procedimentos judiciais liderados pelo ativista Max Schrems. Em 10/07/2023, a Comissão emitiu uma nova decisão de adequação considerando válido o "Trans-Atlantic Data Privacy Framework". No entanto, já há informações que que Max Schrems, pela ONG NOYB, deverá novamente questionar a sua legalidade, posto que o problema da lei de vigilância não foi atacado pelos Estados Unidos.

Diante dessa situação, é a transferência internacional de dados para as plataformas de serviços digitais nos Estados Unidos legal e segura?

Enquanto não houver decisão invalidando o "Trans-Atlantic Data Privacy Framework", as transferências de dados podem se dar ao seu abrigo. No entanto, sendo declarada a sua ilegalidade, as transferências de dados resultarão no incumprimento do RGPD. Vale ressaltar, que, neste caso, considerando a falta de garantia dos Estados Unidos ao respeito à proteção de dados dos cidadãos europeus, cláusulas-tipo também não serão suficientes para atribuir legalidade à referida transferência internacional de dados.

Por fim, são grandes os desafios de empresas europeias dependentes dos serviços digitais de plataformas localizadas fora da União Europeia. De forma a buscar a conformidade com o RGPD, recomenda-se a identificação de provedores locais ou de plataformas que se utilizem de servidores localizados na própria União Europeia ou em países com decisões de adequação válidas e com baixo potencial de questionamento.

Quais os temas que importa dar destaque em âmbito RGPD no setor segurador para o ano de 2024?

Sónia Neves

Data Protection Officer na Zurich Portugal

Zurich Portugal

Tive a oportunidade de, no passado dia 24 de janeiro, a convite do Prof. Dr. Barreto Menezes Cordeiro, do Prof. Dr. Diogo Pereira Duarte e do Prof. Dr. Francisco Rodrigues Rocha participar na Mesa Redonda da V Edição do Curso de Pós-Graduação Avançada em Direito da Proteção de Dados na Faculdade de Direito de Lisboa.

Por essa ocasião, relatei a minha experiência profissional, tendo abordado dois temas que julgo estarem presentes no dia a dia dos Encarregados de Proteção de Dados Pessoais (DPO's), para as organizações, do setor segurador, em âmbito de proteção de dados pessoais, durante o ano de 2024.

O primeiro tema, foi o da Transferência de Dados para Fora da União Europeia e o 2.º tema, o dos Dados Sintéticos.

Relativamente ao 1.º tema, a Transferência de Dados para Fora da União Europeia, o que considero ser relevante?

Qualquer transferência de dados deve ser analisada, seja do ponto de vista técnico como organizacional. Porém quando estejamos perante a transferência para fora da União Europeia, principalmente em empresas multinacionais, o tema toma outras proporções pois existem salvaguardas adicionais que devem ser acauteladas.

Claro está que estas salvaguardas surgem por se considerar

não existir o mesmo nível de proteção que existe na Europa, onde se aplica o Regulamento Geral sobre a Proteção de Dados (RGPD) e daí ser necessário estabelecer determinados critérios, normas, instrumentos que permitam que essa transferência de dados seja efetuada em modos idênticos à União Europeia e assim se protejam os dados pessoais.

Ao longo do tempo (2016 com o *Safe Harbour* e depois em 2020 com o *Privacy Shield*) existiram várias tentativas para regular estas transferências de dados, sendo que somente a 7 de outubro de 2022 se vislumbrou uma possível solução. Nesta data, Joe Biden, Presidente dos Estados Unidos da América emitiu uma Ordem Executiva para regular / dar resposta às questões levantadas pelo Tribunal de Justiça da União Europeia relativamente a esta matéria.

Até este período, as empresas (independentemente do setor) deveriam vincular-se nos termos das cláusulas contratuais-tipo da Comissão Europeia, conjuntamente com uma análise à transferência de dados em concreto, tendo em vista verificar a suficiência das mesmas - isto porque, as cláusulas contratuais-tipo devem ser acompanhas de outras medidas – somente a assinatura não é suficiente – haveria que analisar o regime jurídico do país do importador, de modo a verificar se poderá levar a cabo tudo o que está descrito nas cláusulas. Recordo assim, o exemplo do ocorrido com o Instituto Nacional da Estatística que é um excelente *case study* para este tema (ver link INE multado em 4,3 milhões de euros por causa dos Censos 2021 – ECO (sapo.pt), para mais informações).

Após esta Ordem Executiva, mais concretamente a 10 de julho de 2023, surge então o *EU-U.S. Data Privacy Framework* (DPF) ou Decisão de Adequação para a Transferência de Dados Pessoais entre os EUA e a UE (DA), que se traduz na prática no seguinte: os dados pessoais podem fluir em segurança da União Europeia para as empresas dos EUA sem se ter que implementar salvaguardas adicionais de proteção de dados. Para que isto aconteça, conforme estabelecido pelo DPF ou DA, é necessário 2 requisitos: 1- serem prestadores de serviços (entidades públicas e/ou privadas) certificados no Quadro de Privacidade dos Dados Pessoais da UE-EUA e 2- estarem inscritos no Departamento do Comércio dos EUA ("DOC").

Consequentemente, com estes pressupostos reunidos, os 27 Estados da União Europeia (e ainda: Noruega + Islândia + Liechtenstein + Andorra + Argentina + Canadá (organizações comerciais), Ilhas Faroé + Guernsey (Normandia) + Israel + Ilha de Homem (RU) + Japão + Jersey + Nova Zelândia + República da Coreia + Suíça) existindo partilha/transferência de dados nos tratamentos dos seus serviços/operações/atividades com os EUA, não será necessário aplicar salvaguardas adicionais em âmbito RGPD, porque as empresas pertencentes no DPF ou DA, cumprem com os princípios idênticos ao RGPD no tratamento de dados pessoais o que significa que respeitam e salvaguardam um extenso conjunto de obrigações de privacidade e de segurança de dados, em tudo similar ao RGPD.

Este enquadramento fica ainda mais reforçado com a existência de um novo sistema de recurso para investigar e resolver reclamações dos europeus, titulares dos dados, sobre o acesso aos dados pelas entidades dos EUA, que inclui um Tribunal de Revisão de Proteção de Dados (DPRC) e ainda a possibilidade de existir reclamação diretamente para a autoridade de controlo – Comissão Nacional de Proteção de Dados (CNPD) - bem como a investigação por "Civil Liberties Protection Officer of the Diretor of National Intelligence" – organizações certificadas pelo DPF ou DA.

Posto isto, a melhor prática, num tratamento de dados, aquando da presença de transferência de dados pessoais para fora da União Europeia, com os EUA, o primeiro passo a dar, sugiro que seja a consulta/verificação se a empresa/organização/parceiro se encontram identificados/validados no Data Privacy Framework. Se a resposta for afirmativa, sabemos que se aplicam as regras/salvaguardas supramencionadas e pode-se avançar com a transferência. Caso contrário, haverá que adotar as cláusulas contratuais-tipo da Comissão Europeia, conjuntamente com uma análise à transferência de dados em concreto, para avaliar/ verificar a suficiência das medidas adotadas.

Sobre este tema, importa dar nota que a 24 de abril de 2024 surgiram informações acerca dos modelos de formulários de reclamação para facilitar a implementação dos mecanismos de reparação/reclamação ao abrigo do DPF ou DA. Caso estejam interessados/as podem consultar os mesmos no link EU-US Data Privacy Framework Template Complaint Form for Submitting Commercial Related Complaints to EU DPAs | European Data Protection Board (europa.eu), e obter mais informações. Por último, importa referir que estes formulários serão somente para reclamações relativas às respetivas competências - segurança nacional ou fins comerciais - e para dados transmitidos após 10 de julho de 2023.

Passando ao 2.º tema, isto é, aos Dados Sintéticos qual a sua importância nos dias de hoje relativamente à proteção de dados pessoais?

Para além desta questão, existem também outras questões adjacentes, de tão ou mais relevância, que nos permitem entender o interesse de estes dados também serem analisados à luz do RGPD. Em concreto: O que se entende por dados sintéticos? E porque ainda se vê pouca utilização destes dados? Estes dados, serão a solução para o atual enquadramento legislativo/regulamentar?

Uma das diversas definições largamente utilizada, e que poderá auxiliar na resposta às nossas questões, menciona que "são dados, criados artificialmente, não gerados por eventos reais. Algoritmos de *machine learning*, plataformas de Inteligência Artificial (IA) que aprendem com os dados reais e produzem depois versões sintéticas desses mesmos dados, despersonalizando-os totalmente." Ou seja, serão "conjuntos de dados seguros e compatíveis com a privacidade" utilizados em "processos de desenvolvimento e teste de software", que permitem fornecer "produtos robustos e confiáveis aos

clientes", que respeitam as regras do RGPD.

Atualmente, sabe-se que *fintechs*, *healthtechs*, o setor financeiro e, em particular, o setor dos seguros, já vão recorrendo, utilizando estes dados… porém também sabemos que os mesmos não são amplamente utilizados porque os dados sintéticos são gerados por IA, que no patamar que se encontra no início de 2024, poderá eventualmente criar enviesamento de dados e assim retirar a utilidade dos mesmos.

Particularmente no setor dos seguros, que é onde exerço atualmente as minhas funções, verifico uma constante preocupação em respeitar o RGPD, em perceber como se podem utilizar os dados pessoais, dados de saúde, sem afetar a privacidade/liberdade das pessoas.

Em paralelo, existe a necessidade de criar produtos/serviços inovadores que permitam ir ao encontro da necessidade das pessoas e das diversas situações que pretendem subscrever produtos/serviços e/ou realizar uma simulação. E talvez a solução fosse a utilização destes dados sintéticos. Porém, como já referi, surgem dúvidas nesta matéria, e que consequentemente, origina que o processo de criação/inovação pare.

Todavia, na presente data, já começam a existir projetos com o objetivo de trazer certeza/segurança jurídica a estes processos, à utilização destes dados, através da certificação de plataformas de IA, como é o caso por exemplo do Projeto AICeBlock – Artificial Intelligence Certification through the Blockchain, um projeto de investigação do *Fraunhofer Portugal AICOS*, apoiado pela Imprensa Nacional Casa da Moeda.

Aconselho a consulta do link *AICeBlock*: o projeto que vai certificar inteligência artificial através de blockchain foi distinguido no Prémio IN3+ - UPTEC - *Business and Innovation Hub*, de modo a perceberem qual o trabalho que está a ser realizado, com especial destaque para o seguinte: "Esta plataforma poderá servir para suportar qualquer tipo de aplicação baseada em IA, quer ao nível de treino, quer em produção. No entanto, a sua necessidade é mais evidente em áreas críticas como a saúde ou com elevados requisitos de segurança. Além disso, também ganha especial relevo em casos de desenvolvimento colaborativo — como na Administração Pública, por exemplo. Estes domínios têm requisitos sensíveis e inflexíveis. Ao dotar um novo produto de IA com um selo que garante que este pode ser auditado, com as suas decisões individuais rastreadas, ao mesmo tempo que facilita o cumprimento de normas como o RGPD, ou a inclusão de camadas de interpretação, o *AICeBlock* aumenta a confiança dos utilizadores no produto."

Acredito que num futuro próximo, este projeto será replicado por diversas empresas de modo a trazer principalmente segurança jurídica, assegurando que os dados presentes nas plataformas de IA cumprem com os requisitos e normas do RGPD e assim teremos o melhor dos dois mundos, isto é, teremos a possibilidade dos diversos negócios evoluírem, com produtos

inovadores sem afetar a esfera jurídica dos titulares dos dados, respeitando os direitos legais estabelecidos tanto para a reserva da intimidade da vida privada como principalmente para a proteção dos dados pessoais.

ZURICH

Seguros a favor de novos projetos

Consulte um mediador Zurich
ou visite-nos zurich.com.pt
e peça uma simulação.

Para que tudo corra bem.

Portugal está mais seguro desde 1918

Fonte de Licitude na AP

José António Rajani Oliveira Dias

Associado 232

APDPO

Com o advento do Regulamento Geral sobre a Protecção de Dados, vulgo, RGPD, as entidades responsáveis pelo tratamento de dados de terceiros, viram-se confrontadas com um conjunto de regras, vinculativas, restringindo o livre tratamento que grassava no comércio e na actividade das relações jurídicas, estabelecidas, no sector privado, entre fornecedor de produtos ou serviços e clientes, e no sector público, entre administração e administrado.

Em bom rigor, o sector público já tinha, desde o texto constitucional, ao CPA, passando pelo CCP, um conjunto de regras vinculativas, onde a discricionariedade não tinha espaço.

Mas no sector privado as coisas eram um pedaço "*laissez, fair, laissez passer*", numa dinâmica, quase de intrusão e esbulho de dados pessoais, muitas vezes mesmo contra a vontade do respectivo titular dos dados, quase sempre subordinados a objectivos de lucro fácil, com matéria-prima gratuita, por parte das organizações responsáveis pelo tratamento.

Tendo sido aprovado o RGPD em 2016, altura em que adquiriu a sua **validade**, só em 25 de Maio de 2018, o RGPD adquiriu a sua plena **eficácia**, em toda a União Europeia, após 2 anos de *vacatio legis*, e, diferentemente de uma directiva europeia, que carece sempre de transposição através de acto legislativo nacional, um regulamento comunitário, é de aplicação directa, como foi o caso do RGPD.

A Lei nº 58/2019, de 8 de Agosto, tem sido objecto de muita confusão, na medida em que é, erradamente, vista, como a transposição nacional do RGPD, quando afinal é apenas o cumprimento do Artigo 84º do RGPD, que atribui às autoridades nacionais a competência para o estabelecimento do quadro sancionatório do respectivo País, reconhecendo que cada caso é um caso. Sucede que, para alguns, esta Lei nacional foi muito mais além do

que devia, e a mesma mereceu, da autoridade nacional portuguesa, censura, deliberando esta, pela não aplicação de determinadas normas do diploma, algo que ulteriormente será objecto de outro artigo, em próxima edição.

Aqui chegados, mal ou bem, mais rápido, nuns casos, menos noutros, a verdade é que o Artigo 6º do RGPD, passou a nortear as actuações de uma multiplicidade de responsáveis de tratamento de dados pessoais, sem cuidar, mesmo em sede de assessoria e consultoria em razão de matéria, das diferenças entre o sector privado e o sector público, e isso redundou numa disseminação de práticas de tratamento escorando-se na primeira fonte de licitude – o **Consentimento**.

O consentimento, como fonte de licitude para o tratamento, transformou-se numa panaceia, tipo *Melhoral*, dá para tudo, nem faz bem nem faz mal, á cautela, aplica-se em todos os tratamentos.

Particularmente preocupante, é o caso do sector público. E neste, porque é o universo que mais me diz respeito, as autarquias locais, e nestas as freguesias, escopo da minha actividade no domínio do RGPD.

O consentimento, como fonte de licitude, para tratamento de dados, numa freguesia, terá uma aplicação absolutamente residual, no conjunto de serviços prestados por uma freguesia. Só por completo desconhecimento quer do RGPD quer da especificidade de uma autarquia, e seu enquadramento jurídico, se pode ignorar isto.

Em 2023, tendo sido contratado pela Associação Nacional de Freguesias (ANAFRE), para leccionar formação em freguesias, cobrindo todas as delegações regionais da ANAFRE, este aspecto foi um dos que me mereceu mais atenção, face á constatação do erro, grosseiro, em que, um pouco por todo o lado, laboravam as freguesias, não por culpa própria, mas por culpa alheia, dos tais especialistas que transportam para o sector público, as práticas e metodologias privadas, sem cuidarem das especificidades.

Em matéria de licitude de tratamento de dados pessoais, numa freguesia, e na esmagadora maioria dos casos, aplica-se a alínea c), do Artigo 6º do RGPD, ou seja, o cumprimento de obrigação jurídica.

Aliás, existe um paralelo, entre esta base legal, e o Princípio da legalidade, plasmado no Código do Procedimento Administrativo, a que toda a administração pública está vinculada.

Este princípio do CPA impõe que um ente público aja estritamente dentro dos limites da legalidade, de tal forma que não estando prevista a prática de determinado acto, é vedada a sua prática, ao contrário do privado onde tudo quanto não seja proibido é lícito.

Deste modo o princípio da legalidade e a prática de uma obrigação jurídica andam de mãos dadas, existindo, pois, uma completa complementaridade entre CPA e RGPD.

Vejamos um caso pratico: se um freguês se deslocar aos balcões de uma freguesia a fim de requerer um atestado de situação

económica, a freguesia, atenta á sua competência territorial, é obrigada a fornecer esse atestado. Para o efeito precisa de recolher determinados dados do freguês, desde logo a sua identificação, a fim de dar início ao processo. Agora imagine-se que os serviços lhe pedem para preencher um consentimento para tratamento dos seus dados, e o freguês não dá consentimento para a recolha e tratamento do seu número de cartão de cidadão… inviabiliza a finalidade em causa.

Ou se tendo iniciado o processo, este chega á fase de deferimento, mas o freguês, fazendo uso da prerrogativa associada ao consentimento, revoga o mesmo, na parte referente ao nº do cartão de cidadão, isso inviabiliza a emissão do atestado, onde forçosamente terá de constar a identificação, completa do freguês.

A pratica de actos administrativos, numa freguesia, ou em qualquer outro serviço público, implica, obrigatoriamente a recolha de certos dados, desde logo a completa identificação do cidadão, sem os quais o cidadão não consegue atingir a finalidade pretendida, logo está obrigado a fornecer esses dados, e com isso lá se vai uma das características do Consentimento, o de ser livre.

Claramente o consentimento não se mostra adequado para a emissão de atestados, os quais são uma boa parte dos serviços de uma freguesia, mas não só, isto acontece também com as certidões, as licenças, a concessão de apoios sociais, e por aí fora.

Percebe-se, assim, de forma cristalina que nas freguesias e nos municípios, o que reina é a fonte de licitude do **cumprimento de obrigação jurídica**.

Acresce quem quando falamos de **freguesias** e **municípios**, estamos a falar de uma administração pública, ESPECIAL, porque descentralizada, contrariamente á administração pública desconcentrada, logo também, aqui, temos de atentar ás especificidades próprias das autarquias locais, que não são, nem direcções regionais, nem ministérios, e onde a disseminação de poderes, por via dos institutos de delegação de poderes e de subdelegação de poderes, a que se somam a distribuição de funções legais, e tarefas, impõem um rigoroso conhecimento do universo autárquico.

O exercício do direito ao apagamento

Fernanda Fragoso

E.P.D. SCML

Vice-presidente da APDPO

O Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – RGPD, foi publicado no Jornal Oficial da União Europeia, em 4 de maio de 2016 e entrou em vigor vinte dias depois (artigo 99º, nº1, do RGPD).

A data de 25 de maio de 2018 determina a aplicabilidade do Regulamento Geral sobre a Proteção de Dados (artigo 99º, nº2), em concreto a produção de efeitos obrigatórios em todos os Estados-Membros, o que significa que entre maio de 2016 (entrada em vigor) e maio de 2018 (produção de efeitos), o RGPD já se aplicava, mas não tinha carácter obrigatório.

O exercício do direito ao apagamento, por parte do titular dos dados pessoais pode retroagir à informação com dados pessoais produzida antes da entrada em vigor do RGPD, em maio de 2016, desde que o titular o requeira fundamentadamente e se verifiquem as condições do direito ao apagamento. Conforme dispõe o Considerando 65 do RGPD: "Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto."

O titular dos dados deve fundamentar o pedido, indicando as razões por que pretende apagar os dados pessoais e se são todos ou só alguns. Veja-se, a este propósito,

o link: https://www.cnpd.pt/cidadaos/direitos/direito-ao-apagamento-dos-dados/

O artigo 17º do RGPD, ao consagrar o direito ao apagamento dos dados, também designado por "direito a ser esquecido" permite que o titular dos dados o possa exercer, no âmbito dos motivos elencados no nº1 deste artigo. O tratamento dos dados pessoais que subsista, por parte do responsável pelo tratamento, após o titular dos dados requer legitimamente o seu apagamento, consubstancia uma violação do RGPD.

Contudo, quando se observam os limites do artigo 17º, nº3, a conservação dos dados pessoais pelo responsável pelo tratamento é lícita, conforme decorre, também, do Considerando 65 do RGPD.

Importa, ainda, assinalar o Considerando 67 do RGPD, que dispõe: "Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados."

O direito ao apagamento dos dados pessoais, é um direito novo do titular, introduzido pelo RGPD e surge da necessidade do direito a ser esquecido em especial na informação tratada por via eletrónica, pelo que o exercício deste direito vem reforçar a privacidade do titular dos dados no universo digital, em particular na internet, dada a facilidade de acesso aos dados quando os dados tenham sido tornados públicos.

O artigo 19º, do RGPD, determina, nas situações em que se opera o apagamento dos dados pessoais, o dever do responsável pelo tratamento comunicar tal facto a cada destinatário a quem os dados tenham sido transmitidos. Esse dever só não é exigível nos casos onde tal comunicação se revele impossível ou desproporcionada.

Da articulação do disposto no artigo 5º, nº1, alínea e), do RGPD, com o artigo 21º, da Lei nº58/2019, de 8 de agosto, resulta que o prazo de conservação dos dados pessoais será:

- o que estiver fixado por norma legal ou regulamentar;
- o que se revele necessário para a finalidade do tratamento;

- o que se verificar enquanto decorrer o prazo de prescrição dos direitos.

Constitui obrigação do responsável pelo tratamento a comunicação ao destinatário de que procedeu em conformidade com o pedido de apagamento (artigo 19º, do RGPD).

Quando se opera o exercício do direito ao apagamento dos dados?

Nos termos do artigo 17º, nº1, do RGPD, o direito ao apagamento requerido pelo titular dos dados deve ser operacionalizado, sem demora injustificada, nas seguintes situações:

a) Quando os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

b) Quando o titular dos dados retira o seu consentimento e não exista outro fundamento jurídico para o referido tratamento;

c) Quando exerce o seu direito de oposição, nos termos do artigo 21º, do RGPD, e não existem interesses legítimos prevalecentes, que justifiquem o tratamento, por parte do responsável pelo tratamento;

d) Se os dados pessoais forem tratados ilicitamente;

e) Caso exista uma obrigação jurídica, de apagamento dos dados, decorrente do direito da União ou do direito nacional a que o responsável pelo tratamento esteja sujeito.

f) Quando se trate de dados pessoais recolhidos no contexto da oferta de serviços da sociedade de informação, nos termos do artigo 8º, nº1, do RGPD.

O apagamento dos dados pessoais só não será efetuado, pelo responsável pelo tratamento, nos seguintes casos:

a) Exercício da liberdade de expressão e de informação;

b) Cumprimento de uma obrigação legal;

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9º, nº2, h) e i) e nº3, do RGPD;

d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89º, nº1 do RGPD;

e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O apagamento dos dados "sem demora injustificada" a que se refere o corpo do artigo 17º, nº1, significa que o mesmo terá de ser executado no prazo de um mês, a contar da data da receção do pedido, prazo que poderá ser prorrogado até dois meses quando se verifique a especial complexidade do pedido e o número de pedidos (artigo 12º, nº3, do RGPD).

Em conformidade, verifica-se que o cumprimento, por parte do responsável pelo tratamento, do pedido formulado pelo titular dos dados no exercício do seu direito ao apagamento, tem de ser aferido casuisticamente para verificação da conformidade com os princípios

relativos ao tratamento dos dados pessoais, constantes no artigo 5º, do RGPD, bem como para uma correta identificação da base de licitude que motivou a recolha ou o tratamento dos dados que o titular pretende eliminar.

Liderlink
Business Solutions

COLOCAMOS A **CIBERSEGURANÇA EM PRIMEIRO PLANO**

Na **LIDERLINK Business Solutions** entendemos a importância de proteger informação e de atender a regulamentações rigorosas de privacidade de dados.

Quem Somos?

Com uma reputação sólida no setor de cibersegurança e um compromisso inabalável com a privacidade de dados, a **LIDERLINK Business Solutions** é a parceira ideal para profissionais que procuram proteger organizações contra ameaças externas.

Como Ajudamos?

Apresentamos sempre uma abordagem personalizada que combinamos com as mais recentes inovações em segurança de dados para garantir uma protecção eficaz dos dados das organizações.

Os Nossos Serviços

Soluções Avançadas

Oferecemos um conjunto completo de soluções de cibersegurança como detecção de ameaças, monitorazação de redes, entre outros.

Segurança Cloud

Mantemos dados seguros na com soluções de segurança personalizadas para ambientes na Cloud.

Recuperação de Dados

Desenvolvemos planos de recuperação personalizados para garantir que as organizações recuperam de eventos inesperados.

FALE CONNOSCO

282 475 763

geral@liderlink.pt
www.liderlink.pt

Quinta do Alto,
Lote 21,
8400-142 Lagoa


APDPO
PORTUGAL