DPO mag

EDIÇÃO Nº 10
JUL / 25

APDPO PORTUGAL

www.dpo-portugal.pt

DPO mag

EDIÇÃO Nº 10
JUL / 25

APDPO PORTUGAL

www.dpo-portugal.pt

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


APDPO
PORTUGAL

Mensagem da Diretora

Bem-vindos à **DPO Magazine n.º 10**!

Depois de um semestre ausentes, por não termos conseguido granjear o número mínimo de artigos para publicação, voltamos muito satisfeitos por reunirmos nesta edição valiosos conhecimentos, pensamentos e experiências!

A primeira palavra destas breves linhas é, pois, dedicada aos Autores desta edição, aos quais, a Todos e a cada Um, agradecemos penhoradamente a partilha e dedicação.

É por Eles e para Todos que este projeto associativo continua a fazer sentido e merece toda a atenção e cuidado da Direção da APDPO, que continua comprometida e empenhada em priorizar a temática da proteção de dados pessoais.

O calendário traz-nos mais um dia 25 de maio, que é a oportunidade ideal para assinalar a importância da proteção de dados e comemorar a entrada em aplicação do RGPD, que, neste ano de 2025, completa o 7.º aniversário!

Numa altura em que as notícias nos dão a novidade de que a Comissão Europeia prepara alterações ao Regulamento Geral sobre a Proteção de Dados, visando em especial a redução de encargos para as pequenas e médias empresas - sem comprometer a proteção da privacidade, sublinham, parece-nos que não será demais recordar a necessidade de garantir os princípios fundamentais que têm norteado as legislações nesta matéria!

Aventam-se alterações no que toca ao RAT (art. 30.º), mas não só. Uma das críticas vindas da UE respeita à aplicação desigual e à fragmentação legislativa, que trazem incerteza jurídica, designadamente no regime aplicável aos menores. Os elevados custos de conformidade também estão a ser amplamente criticados.

Certo é que estas alterações agora faladas surgem num contexto de crescente pressão política, em que a estratégia é para reforçar a competitividade da economia europeia, designadamente através de medidas de simplificação administrativa, e em que é apontado o impacto negativo da regulamentação europeia na capacidade de inovação das empresas, sendo o RGPD visto como um dos principais entraves ao empreendedorismo e ao desenvolvimento de tecnologias emergentes, incluindo soluções de cibersegurança e inteligência artificial.

Esperemos que as propostas da Comissão não aligeirem a proteção que Todos merecemos! Entretanto lançada fica a décima edição da revista da APDPO.

Boas leituras e vemo-nos na próxima edição!

Inês Oliveira

Presidente da Direção da APDPO

Diretora da DPO Magazine

Conteúdo

A Importância da Interação entre o DPO e as unidades de GRC

O papel do Encarregado de Proteção de Dados (***Data Protection Officer*** **- DPO**) assume uma relevância central na salvaguarda da privacidade e no cumprimento das regulamentações de proteção de dados, com destaque para o Regulamento Geral sobre a Proteção de Dados (RGPD). Cabe ao **DPO** assegurar que a organização cumpre integralmente as obrigações legais em matéria de proteção de dados pessoais. No entanto, para que essa função seja desempenhada de forma eficaz, é imprescindível que o **DPO** mantenha uma interação estreita com a unidade responsável de ***Governance, Risk, and Compliance*** **(GRC)**. Este artigo explora a importância desta colaboração e a correlação entre o **RGPD**, a Diretiva **NIS2** e o ***AI Act***, particularmente no que concerne à privacidade e à resiliência da proteção de dados.

1. Governança, Risco e Conformidade (GRC) e o Papel do DPO

O conceito de ***Governance, Risk, and Compliance*** **(GRC)** abrange um conjunto de práticas que integram as funções de governança corporativa, gestão de riscos e conformidade regulatória. Os *stakeholders* envolvidos desempenham um papel essencial na garantia de que a organização opera em conformidade com a legislação aplicável, enquanto adota práticas adequadas de gestão de riscos. A articulação entre o DPO e o(s) departamento(s) de GRC é, portanto, determinante para a implementação eficaz de uma estratégia sólida de proteção de dados, uma vez que ambos os domínios partilham objetivos complementares:

- **Governança**: O DPO colabora com o GRC para assegurar que a governança da informação esteja alinhada com as exigências legais em matéria de proteção de dados. Assim, o DPO supervisiona a implementação de políticas de proteção de dados que sejam coerentes com a estrutura de governança da organização.

- **Risco**: A identificação e mitigação dos riscos relacionados com a privacidade são componentes cruciais da função do DPO. O departamento de GRC, através da sua estrutura de gestão de riscos, facilita este processo ao fornecer uma base para identificar, avaliar e mitigar os riscos associados ao tratamento de dados pessoais. A cooperação entre o DPO e o GRC permite uma abordagem proativa na prevenção de incidentes de violação de dados.

- **Conformidade**: O DPO tem a responsabilidade de assegurar que a organização cumpre as disposições do RGPD e outras normas relativas à proteção de dados. O departamento de GRC, por seu lado, garante que a conformidade global da organização

com todas as regulamentações é monitorizada de forma contínua, contribuindo assim para evitar sanções legais e proteger a reputação institucional.

2. A Correlação entre o RGPD, a NIS2 e o *AI Act*

Com a crescente relevância das questões de cibersegurança, a Diretiva NIS2 e o *AI Act* assumem uma importância crescente, complementando o RGPD em domínios específicos. A interação entre estas três regulamentações tem impacto direto na proteção da privacidade e na resiliência dos sistemas de proteção de dados.

2.1. RGPD (Regulamento Geral sobre a Proteção de Dados)

O RGPD constitui o pilar da regulamentação em matéria de proteção de dados pessoais na União Europeia. Este regulamento estabelece os direitos fundamentais dos indivíduos relativamente aos seus dados pessoais e define obrigações rigorosas para as organizações quanto à forma como devem tratar e proteger esses dados.

2.2. NIS2 (*Network and Information Security Directive*)

A Diretiva NIS2 visa reforçar a segurança das redes e dos sistemas de informação na União Europeia, impondo requisitos específicos em termos de cibersegurança e notificação obrigatória de incidentes. Embora o foco da NIS2 seja, primariamente, a segurança da informação, existe uma interseção clara com a proteção de dados, uma vez que a segurança da informação constitui um alicerce para a proteção eficaz dos dados pessoais.

2.3. *AI Act* (*Artificial Intelligence Act*)

O *AI Act* visa regulamentar o desenvolvimento e a utilização de sistemas de Inteligência Artificial (IA) na União Europeia, assegurando que estes são concebidos e aplicados de forma ética, segura e em conformidade com os direitos fundamentais, incluindo a proteção de dados. Considerando que muitos sistemas de IA implicam o processamento de grandes volumes de dados pessoais, é fundamental que tais operações respeitem os princípios estabelecidos pelo RGPD e que os riscos associados à IA sejam adequadamente geridos.

3. Matriz de Correlação entre o RGPD, NIS2 e *AI Act*

A matriz abaixo demonstra a correlação entre o RGPD, a NIS2 e o *AI Act*, salientando as suas implicações na privacidade e na resiliência da proteção de dados.

4. Conclusão

A colaboração estreita entre o DPO e as unidades de GRC é essencial para garantir que as organizações estão devidamente equipadas e preparadas para enfrentar os desafios relacionados com a proteção de dados e a cibersegurança no contexto europeu. A interação eficaz entre o RGPD, a NIS2 e o *AI Act* é crucial para assegurar que as organizações não só cumprem as suas obrigações legais, mas também reforçam a resiliência e a privacidade dos dados num ambiente cada vez mais digital e interconectado. A sinergia entre estas

regulamentações, juntamente com a cooperação interdepartamental, revela-se, assim, um fator determinante para a construção de uma estrutura robusta de governança e proteção de dados, capaz de responder às exigências legais e às ameaças emergentes.

Mário Peixinho

Data Privacy Advisor

HITO Innovation Group

Aspectos	RGPD	NIS2	AI Act
Privacidade	Estabelece os direitos dos indivíduos e impõe obrigações rigorosas para a proteção de dados pessoais.	Reforça a segurança dos sistemas que protegem os dados pessoais, mitigando o risco de violações.	Garante que a IA trata os dados pessoais de forma ética e em conformidade com o RGPD.
Resiliência	Foca-se na proteção e resiliência dos dados pessoais contra acessos não autorizados e violações.	Impõe medidas de cibersegurança que garantem a resiliência dos sistemas de informação que armazenam e processam dados pessoais.	Promove a resiliência nos sistemas de IA, prevenindo falhas que possam comprometer a proteção de dados pessoais.
Conformidade	Exige conformidade rigorosa com a legislação de proteção de dados.	Requer que as organizações cumpram normas rigorosas de segurança da informação que suportam a proteção de dados pessoais.	Regula o uso de IA de modo a garantir a conformidade com as normas de privacidade e proteção de dados.

O Papel Estratégico do DPO na Era da Inteligência Artificial

Com a rápida ascensão da Inteligência Artificial (IA) no ambiente corporativo, as empresas estão a adotar tecnologias como chatbots, modelos de linguagem de grande escala (LLMs) e sistemas preditivos para otimizar os seus processos de negócio e tomar decisões automatizadas. No entanto, este avanço tecnológico traz consigo riscos significativos, especialmente no que diz respeito à conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD).

Nesse contexto, o DPO (*Data Protection Officer*) assume um papel de protagonista, sendo responsável por garantir que o crescente uso de IA nas empresas respeite as exigências legais. No entanto, esse papel não se limita à conformidade regulatória, podendo tornar-se uma oportunidade ideal para o profissional se posicionar como um catalisador que gera valor estratégico dentro da organização. De facto, a conformidade bem executada torna-se um diferencial competitivo, permitindo que as empresas alinhem o uso de IA com as expectativas crescentes de transparência e responsabilidade.

Um dos principais desafios que os DPOs começam a enfrentar, e que tende a crescer exponencialmente, é garantir que as ferramentas de IA utilizadas pela empresa, sejam desenvolvidas internamente ou contratadas de terceiros, estejam em conformidade com o Artigo 5.º do RGPD, que estabelece princípios como a limitação de finalidade e a minimização de dados. Ferramentas como os LLMs requerem uma supervisão constante, pois utilizam grandes volumes de dados para treino e operação. Cabe ao DPO garantir que esses dados sejam tratados de maneira ética e segura, evitando o seu uso indevido.

Além disso, o *AI Act*[1], que entrou em vigor em agosto de 2024, trouxe novos pontos de atenção para o DPO, principalmente no que diz respeito às tecnologias de IA classificadas como de "alto risco", que deverão passar por auditorias e avaliações de impacto regulares. Entretanto, a implementação deste regulamento será feita de forma gradual, com marcos importantes a serem observados:

- A partir de fevereiro de 2025, será aplicada a proibição contra IAs de "risco inaceitável";
- Em agosto de 2025, entram em vigor as regras para os modelos de IA de propósito geral e as autoridades de fiscalização começam a atuar;

[1] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689

- Em agosto de 2027, serão implementadas as regras para a classificação das IAs de "alto risco".

Esses prazos oferecem aos DPOs uma oportunidade para planear e liderar de forma proativa a adaptação da empresa.

Outro papel fundamental do DPO é assegurar que os titulares de dados estejam plenamente informados sobre o uso de IA em processos que possam afetá-los diretamente, como decisões de crédito ou processos de recrutamento. De acordo com o Artigo 6.º do RGPD, o consentimento deve ser livre, informado e explícito. No contexto da IA, essa transparência torna-se ainda mais complexa, pois muitos indivíduos desconhecem que as decisões que os afetam são, total ou parcialmente, automatizadas com IAs. O DPO deve garantir que o consentimento seja obtido e que as informações sejam comunicadas de forma **acessível**, reforçando a confiança entre a empresa e os seus consumidores.

O Artigo 22.º do RGPD dá aos titulares o direito de não se submeterem a decisões inteiramente automatizadas, que possam ter impacto significativo nas suas vidas. Cabe ao DPO assegurar que as empresas que utilizam IA em processos decisórios estejam aptas a fornecer explicações compreensíveis sobre a lógica por trás dessas decisões. A **explicabilidade algorítmica** [2] é fundamental, não apenas para cumprir com as obrigações legais, mas também como uma oportunidade para a empresa demonstrar responsabilidade e transparência, criando uma vantagem competitiva. Empresas que conseguem justificar as decisões de seus processos de negócio de forma clara e assertiva, garantindo que os seus algoritmos não possuem vieses discriminatórios, destacam-se no mercado e ganham a confiança dos consumidores.

A conformidade com o RGPD e o *AI Act* não deve ser vista apenas como uma obrigação legal, mas sim como uma oportunidade estratégica para as empresas se diferenciarem em um mercado cada vez mais competitivo. Ao promover uma cultura de conformidade, ética e inovação responsável, o **DPO transforma-se num ativo estratégico da organização**, ajudando a empresa a mitigar riscos e a conquistar novos negócios. A transparência no uso de IA reforça a confiança dos consumidores, enquanto uma abordagem ética atrai investidores e fortalece a reputação da empresa.

[2] http://dx.doi.org/10.1109/CSR57506.2023.10224998

Assim, o DPO não é apenas um guardião da conformidade, mas também um líder que, ao garantir o uso responsável da IA, posiciona a empresa na vanguarda da inovação pautada na ética e no respeito pelo consumidor. Ao assumir essa postura proativa, o **DPO reforça seu valor como um profissional essencial e distinto no cenário corporativo atual**.

Jackson Barreto

Engenheiro Informático, Jurista, Especialista em Cibersegurança; e professor no Instituto Politécnico de Viana do Castelo (IPVC) e Instituto Politécnico do Cávado e do Ave (IPCA).

DPO & *Marketing*: Uma Aliança Estratégica para a Confiança

Como o Encarregado de Protecção de Dados pode e deve ser um parceiro activo nas estratégias de marketing directo e digital

Os dados pessoais tornaram-se uma matéria-prima essencial para muitas das actividades de marketing e por isso é fundamental que se aprofunde e desenvolva a relação entre os profissionais de marketing e os Encarregados de Protecção de Dados (DPO).

Longe vai o tempo em que a Protecção de Dados era vista como uma série de obstáculos à criatividade, inovação ou eficácia das campanhas.

Hoje, é cada vez mais claro que o verdadeiro marketing de excelência é aquele que assenta na confiança — e esta não se constrói sem privacidade.

Para materializar essa confiança, é preciso mais do que boas intenções e mensagens de marketing vazias. É necessário existir uma **colaboração estreita, efectiva e estratégica entre os Departamentos de *Marketing* e os DPOs**. É vital que ambos falem a mesma linguagem, compreendam os desafios uns dos outros e trabalhem em conjunto desde o primeiro momento de cada acção.

O DPO Como Parceiro e Não Como "Polícia de Serviço"

O Regulamento Geral sobre a Protecção de Dados (RGPD) instituiu o papel do DPO como figura central na supervisão da conformidade com a legislação.

Um DPO que compreenda profundamente as práticas e tecnologias do *marketing* directo e digital tem mais capacidade de orientar, em vez de apenas limitar. Um Departamento de *Marketing* que integre o DPO desde a génese das suas campanhas, ganha em agilidade, segurança jurídica e até em reputação.

Esta relação, bem gerida, transforma o DPO num verdadeiro **aliado estratégico** e não num mero auditor ou corrector *a posteriori*. Esta relação saudável permite poupar tempo, dinheiro, stress e sobretudo potencia os resultados da organização.

***Marketing*: Um Território de Complexidade Tecnológica e Jurídica**

É difícil, mesmo para profissionais experientes, acompanhar o ritmo a que evoluem as ferramentas e canais de *marketing* digital. Plataformas de automação, sistemas de CRM, segmentação por dados comportamentais, *cookies*, *pixels*, publicidade programática, *marketing* em redes sociais, influenciadores, geolocalização e tudo temperado com uma pitada de inteligência artificial.

Isto tudo implica **fluxos complexos de dados pessoais**, muitas vezes tratados por entidades terceiras, em jurisdições distintas, com modelos de negócio opacos.

Neste cenário, a intervenção do DPO torna-se não só útil, mas indispensável. E para que essa intervenção seja eficaz, é necessário que o DPO tenha uma compreensão funcional destas práticas. Perceba como funciona uma campanha de *email marketing* segmentada, o que é uma taxa de conversão, que dados estão a ser utilizados para uma campanha de *remarketing*, ou como se aplica o princípio da

minimização num formulário de geração de leads.

Do Lado do *Marketing*: Vencer a Resistência e Criar uma Cultura de Privacidade

A responsabilidade, claro, não está apenas do lado do DPO. Os profissionais de marketing têm o dever de compreender as bases legais do tratamento de dados, os limites do consentimento, a importância da informação clara e acessível, e o risco reputacional associado a práticas abusivas ou pouco transparentes.

Além disso, devem ser proactivos em envolver o DPO nas decisões. Não para pedir "autorização", mas para construir em conjunto, soluções criativas, eficazes e conformes. A experiência mostra que quanto mais cedo o DPO é envolvido, menos entraves surgem no caminho, e mais coesa e robusta se torna a estratégia.

Privacidade Como Vantagem Competitiva

Num mercado saturado de mensagens, notificações e anúncios, os consumidores começam a distinguir as marcas que respeitam o seu espaço, os seus dados e o seu direito à escolha. A privacidade deixou de ser apenas uma obrigação legal para se tornar num **diferenciador estratégico**.

A transparência, o consentimento, a possibilidade de configurar preferências, a explicação simples sobre o uso dos dados. Tudo isto contribui para construir **relações duradouras e baseadas na confiança**. E quem melhor para garantir que estes princípios estão integrados desde a concepção das campanhas do que o DPO?

Lista *Robinson*: Um Exemplo de Boa Prática em *Marketing* Responsável

Uma das ferramentas que reflecte este compromisso com o respeito pelas preferências dos consumidores é a **Lista de Oposição** (conhecida como Lista *Robinson*), gerida pela AMD. Esta lista permite a qualquer cidadão indicar que **não deseja receber comunicações de *telemarketing* ou *direct mail* (correio endereçado) não solicitadas**, sendo um instrumento de protecção do consumidor e de promoção de práticas mais responsáveis no marketing directo.

A existência e utilização desta lista não deve ser encarada como uma limitação, mas antes como uma oportunidade para as marcas demonstrarem que respeitam verdadeiramente a vontade dos seus públicos. Integrar esta dimensão ética e operacional nas práticas de marketing é, hoje, um sinal de maturidade.

Uma Nova Geração de Profissionais

O futuro do *marketing* passa, inevitavelmente, por uma maior interdisciplinaridade. DPOs que compreendem os objectivos de negócio e as métricas de sucesso; *Marketers* que compreendem os fundamentos da protecção de dados e as implicações legais das suas escolhas.

As Associações profissionais, como a **APDPO e a AMD**, têm aqui um papel fundamental: **promover a formação cruzada**, criar pontes entre comunidades profissionais, partilhar boas práticas e reforçar a ideia de que a privacidade e marketing andam de mãos dadas.

Conclusão

Está na altura de olharmos para esta relação de forma diferente. O DPO não existe para travar a criatividade, mas sim para ajudar a que ela seja segura e duradoura. E o *Marketing* não precisa de viver com dúvidas legais. Pelo contrário, pode e deve ser orientado por princípios de responsabilidade e respeito pelos dados dos consumidores.

***Marketing* e Protecção de Dados não são mundos à parte. São, cada vez mais, dois lados da mesma moeda: a moeda da confiança.**

André Novais de Paula

Presidente

AMD | Associação Portuguesa de Marketing Directo e Digital

Pseudonimização ou Não Psedonimização? Eis a questão!

No passado dia 17 de janeiro, o Comité Europeu para a Proteção de Dados (CEPD) publicou as Orientações 01/2025 sobre a Pseudonimização.

E o que se entende por Pseudonimização? Segundo o Regulamento Geral sobre a Proteção de Dados (RGPD), por Pseudonimização considera-se a salvaguarda que pode ser adequada e eficaz para o cumprimento das obrigações de proteção de dados, traduzindo-se num "tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável" – art.º 4/5 do RGPD.

Contudo, esta salvaguarda, apesar de estar referenciada no RGPD, desde a sua criação até à presente data, ainda levanta muitas dúvidas sobre a sua aplicação e/ou utilização na prática. Porque será?

Para perceber, importa recordar o caso Single Resolution Board (SRB) vs CEPD, que remonta a setembro de 2017 e a novembro de 2019, e que diz respeito à situação do SRB ter fornecido à Deloitte uma lista de dados, onde se incluía um código alfanumérico para identificar o titular de cada dado, sem o quadro de correspondência. No seguimento, o CEPD recebeu queixas dos titulares desses dados, referindo que o SRB tinha violado as suas obrigações de transparência ao não mencionar a Deloitte entre os destinatários dos seus dados. O CEPD investigou as queixas e, em junho de 2020, sancionou o SRB por transmitir os dados dos titulares à Deloitte sem os informar adequadamente. O SRB na altura recorreu desta decisão ao Tribunal de Justiça da União Europeia (TJUE), apresentando a justificação que os dados pseudonimizados deixam de ser dados pessoais, quando são transformados, encriptados, só podendo reverter essa informação através de informações adicionais e ligar a informação pseudonimizada a dados pessoais. Todavia, uma vez que essa informação adicional existia algures, na situação de serem disponibilizados a terceiro que não a possua (sabe-se que a Deloitte não a dispunha porque o SRB não a forneceu), o CEPD considerou que o SRB não deveria ter atuado dessa forma.

Para o CEPD, haveria a necessidade de ter informado os titulares dos dados de que a Deloitte era uma das «destinatárias» dos seus dados. Na altura, este entendimento ficou conhecido como "interpretação objetiva" dos dados.

No entanto, no caso em questão, o TJUE decidiu que o CEPD deveria ter analisado se a Deloitte teria capacidade para identificar os titulares dos dados. Se a Deloitte não conseguisse reidentificar as pessoas/titulares utilizando os meios ao seu dispor, o conjunto de dados não deveria ser um dado pessoal para a Deloitte.

Caso conseguissem reidentificar as pessoas/titulares considerar-se-ia estar perante dados pessoais. Esta "nova" interpretação foi considerada subjetiva. Nessa altura, o TJUE anulou a sanção e devolveu o processo ao CEPD para reiniciar o processo.

Qual a solução encontrada para este caso? Até à presente data, a decisão deste caso não é pública, porém, existe o entendimento generalizado que com as Orientações 01/2025, pretende-se antecipar a solução, isto é, a clarificação por parte do CEPD do que se entende por pseudonimização e qual a definição e a aplicabilidade da mesma e dos dados pseudonimizados, bem como as suas vantagens, a dias de se conhecer a decisão final, não é inocente.

Assim sendo, das Orientações 01/2025, conseguimos extrair duas regras relevantes, que devem ser tidas em conta, a partir da data de publicação desta documentação. Em concreto, quando se aplica a pseudonimização, os **dados pseudonimizados**, que possam ser atribuídos a uma pessoa singular através da utilização de informações adicionais, continuam a ser informações relacionadas com uma pessoa singular identificável e, por conseguinte, continuam a ser dados pessoais. Com efeito, se os dados puderem ser associados a uma pessoa singular pelo responsável pelo tratamento ou por outra pessoa, continuam a ser dados pessoais e **NUNCA deixam de ser dados pessoais**, independentemente da interpretação que se tenha como aconteceu no passado com o caso SRB. E ainda, com esta salvaguarda **pode-se reduzir os riscos e facilitar a utilização de interesses legítimos** desde que, todos os outros requisitos do RGPD sejam cumpridos, respeitando o propósito inicial de proteção da identificação dos titulares dos dados. Relembro que, para o legislador europeu, esta salvaguarda tem o intuito de ajudar as organizações a cumprir com as suas obrigações relacionadas com a proteção de dados pessoais desde a conceção e por defeito, fazer cumprir com os princípios de proteção de dados, bem como garantir a segurança de informação, a confidencialidade e ainda impedir a identificação não autorizada de pessoas/titulares dos dados.

Posto isto, aconselho a leitura atenta destas Orientações 01/2025, especialmente dos procedimentos e os exemplos referenciados na documentação e se me permitem, sugiro adicionalmente algumas recomendações às organizações, para quem, no seu dia a dia laboral, se depara com a decisão de se optar pela pseudonimização ou por qualquer outra técnica como por exemplo a anonimização dos dados (salvaguarda mais eficaz na proteção dos dados, todavia com maior impacto no negócio).

Em suma, tendo em conta as Orientações 01/2025, caso se opte pelo recurso à pseudonimização, (por exemplo, num sistema informático que comporte [illegible] e tratamento de dados pessoais, se precisa proceder à eliminação de dados pessoais sob uma finalidade que cessou, mas há que manter esses mesmos dados, porque a organização tem que proceder ao tratamento desses dados para outra finalidade que ainda não terminou, de modo a não colocar esses dados pessoais, inacessíveis) os responsáveis pelo tratamento que realizem tratamento de dados pessoais sob pseudónimo/chave informática/identificador, para reduzir os riscos de confidencialidade de alguns ou de todos os dados perante terceiros não autorizados, devem garantir a adoção de medidas que permitam assegurar que os intervenientes no domínio da pseudonimização não possam inverter esta salvaguarda.

Ter presente que, nas Orientações 01/2025, se entende por intervenientes, inclusive terceiros, isto é, colaboradores, empregados, prestadores de serviços, parceiros, etc, que agem no seu próprio interesse e não sob instruções do responsável pelo tratamento.

Caso entrem no domínio da pseudonimização, a fim de evitar a reindentificação de dados pseudonimizados, devem ser tomadas medidas técnicas e organizativas que garantam, em 1.º lugar, que a transformação sob pseudónimo deve ser protegida contra a reversão, escolhendo um desenho ou modelo adequado e garantindo um nível adequado de segurança. Em 2.º lugar, os quase-identificadores devem ser tratados de forma adequada, e obedecendo às regras mencionadas no Ponto 3 das orientações do CEPD. Em 3.º e último lugar, os responsáveis pelo tratamento de dados devem assegurar que os seus pressupostos sobre o âmbito de aplicação do domínio da pseudonimização, sobre a utilização de dados pseudonimizados e sobre a acessibilidade das fontes de informação pertinentes no mesmo, são cumpridos.

Sónia Neves

Data Protection Officer

ZURICH PORTUGAL

Mais do que cobrir riscos, encontramos soluções.

Consulte um mediador Zurich, aceda à App Z4U ou visite-nos em zurich.com.pt.

Para que tudo corra bem.

ZURICH

O Mercado Único Digital e a interoperabilidade administrativa à luz do paradigma *e-Health*

Considerações preliminares

Factual é a ideia de que o desenvolvimento da União Europeia surge alicerçado no Mercado Único Digital (doravante, MUD). Consequentemente, importa analisar o modo como a era digital perpetuou mudanças de paradigma em várias áreas, designadamente na área da saúde. Ora, neste âmbito, o MUD adquire particular relevância, evidenciando utilidade ao nível da interoperabilidade administrativa e da saúde em linha (*e-Health*): fomenta a integração de sistemas de saúde eletrónicos entre os Estados-Membros, permitindo o acesso a dados médicos transnacionais de forma criteriosa e eficiente.

Fácil e rapidamente se percebeu que as medidas implementadas pelos Estados a nível interno não eram suficientes para acompanhar a evolução tecnológica nos diversos domínios da sociedade. Neste seguimento, a União Europeia desenvolveu uma Agenda Digital para a Europa no âmbito da Estratégia Europa 2020, concluindo que o envolvimento das Administrações nacionais e europeias era crucial para a efetividade de um MUD.[1] É, portanto, correto afirmar que este Mercado ambiciona a revitalização de serviços públicos, designadamente pelo seu meio predileto: a interoperabilidade.[2]

Segundo o art. 2º/1 da Decisão (UE) nº 2015/2240 – que estabelece o programa ISA² (*Interoperability Solutions for European Public Administrations*) da União Europeia – interoperabilidade designa a "capacidade de as organizações interagirem de modo a prosseguir objetivos comuns, partilhando informações e conhecimentos, entre as suas políticas e processos de negócio, através do intercâmbio de dados entre os respetivos sistemas de informação".[3] Deste modo, é consensual que o caminho da saúde em linha deve ser o da interoperabilidade, tal como, aliás, ressalva a Diretiva 2011/24/UE: os Estados-Membros devem munir-se de forças e, consequentemente, constituir um arsenal de projetos e sistemas destinados ao combate dos desafios engendrados pela transição digital.[4]

Assim, a emergência de uma era pautada por frenéticos avanços tecnológicos reclama a necessidade de uniformizar soluções legais para

[1] Joana Covelo Abreu, 2017, Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions, UNIO – EU LAW Journal, vol. 3.
[2] Joana Covelo Abreu, 2019, Os Serviços Públicos Digitais na União Europeia: A interoperabilidade Administrativa e a Saúde Administrativa in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov, p. 53
[3] Cfr. Decisão (UE) nº 2015/2240, do Parlamento Europeu e do Conselho, de 25 de novembro, responsável pela criação de um programa relacionado com soluções de interoperabilidade.
[4] Cfr. Diretiva (UE) nº 2011/2014, do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativamente aos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

os problemas por esta acarretados. Aliás, no universo da saúde eletrónica, onde orbitam ferramentas como sistemas de registos de saúde, prescrições eletrónicas e aplicações de rastreamento, suscita-se a questão de saber como serão protegidos os dados pessoais dos doentes.[5]

O paradigma *e-Health*

Efetivamente, nos tempos que correm, o direito à saúde encontra-se numa posição de vulnerabilidade devido a uma panóplia de fatores: os sistemas médicos demonstram uma notória insustentabilidade a nível de gestão financeira, a nível da capacidade de resposta e, ainda, no que concerne às exigências de universalidade e equidade no acesso. Neste sentido, cada vez mais a tecnologia se revela como uma luz ao fundo do túnel, potencializando melhorias na prestação de cuidados médicos: verificou-se uma atualização tecnológica dos hospitais, a introdução de novos mecanismos que permitem diminuir o "erro médico" e o surgimento de inovações como a telemedicina ou a monitorização remota de pacientes. Vivenciamos, portanto, o auge do paradigma *e-Health*, enquanto componente fundamental do MUD e perpetuadora de melhorias na eficiência dos sistemas de saúde dos Estados-Membros.[6]

Neste contexto, domínios como a telemedicina (*e-medicine*) e o atendimento domiciliar eletrónico (*e-home care*) adquirem relevância. A telemedicina consiste na difusão da medicina e dos cuidados de saúde através de sistemas de informação e comunicação (TIC), recorrendo a uma série de instrumentos, como o diagnóstico e a imagem eletrónica (*e-diagnosis* e *e-imaging*) para se fazer valer. Distingue-se, assim, dos tradicionais sistemas de videoconferência pelo uso de dispositivos que permitem uma examinação virtual. E apesar da carência de interação humana direta, a realidade é que a telemedicina impulsiona o cuidado de pessoas vulneráveis que habitam em áreas remotas, assim como a redução de custos, nomeadamente de deslocação.

Por sua vez, o atendimento domiciliar eletrónico refere-se à utilização das TIC na assistência de doentes que escolhem ficar no seu domicílio em detrimento de permanecer num estabelecimento de saúde. Ora, neste seguimento, o *e-health care* permite um certo empoderamento do paciente (*patient empowerment*), destacando a sua autonomia e o seu direito a fazer escolhas relativamente aos cuidados que anseia. Além disso, temos ainda outros domínios em constante aprimoramento: a telecirurgia, que permite aos cirurgiões operar em local remoto com o apoio de instrumentos dotados de inteligência artificial; e a teleradiologia, mediante a qual os hospitais subdesenvolvidos conseguem obter imagens

[5] Anabela Susana de Sousa Gonçalves, 2019, Processing of personal data concerning health under the GDPR in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov, pp. 3-8.
[6] Isa António, 2019, O impacto da tecnologia no setor da saúde e dos direitos fundamentais do doente, in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov, pp. 135-140.

médicas de hospitais mais qualificados, por via eletrónica.[7]

De facto, os cuidados médicos nos Estados-Membros têm evoluído quase à velocidade da luz, sob o efeito de mudanças demográficas, da transição digital e da reconceptualização das políticas de saúde. Urge, portanto, uma ação integrada entre os Estados, designadamente a nível internacional, vocacionada para o desenvolvimento de programas de saúde eletrónica, de modo a alcançar a interoperabilidade de sistemas, bem como a construção de padrões éticos comuns E, efetivamente, a União Europeia já começou a trilhar esse caminho, concretamente por via da brochura informativa de 2019 destinada à exposição de mecanismos passíveis de fomentar a interoperabilidade administrativa no âmbito da saúde em linha: falamos, por exemplo, dos projetos *Smart4Health*, *InteropEHRate* e *openMedicine.*[8]

A digitalização da saúde europeia no cenário pandémico e pós-pandémico: mecanismos e iniciativas

Declarada em março de 2020 pela Organização Mundial da Saúde (OMS), a pandemia da COVID-19 constituiu um dos maiores desafios globais na esfera da saúde pública do século XXI.[9] Note-se que a situação pandémica, além de colocar à prova os sistemas nacionais de saúde, reclamou ainda a importância de respostas articuladas entre os Estados, tendo a digitalização se evidenciado como um mecanismo crucial na gestão da crise. Ora, num contexto de confinamentos generalizados e de rutura dos sistemas de saúde, a União Europeia revelou-se pioneira no recurso a tecnologias digitais para neutralizar a propagação do vírus *SARS-CoV-2*, nomeadamente através da criação de aplicações de rastreio de contactos e de sistemas de informação médica partilhada.

De facto, as aplicações móveis de *smart tracing* e *mHealth* afiguraram-se vantajosas em diversas situações: contribuíram para um aumento da capacidade de resposta médica, aliviando a pressão exercida sobre os profissionais de saúde e possibilitando a colmatação de falhas identificadas na memória humana. Além disso, prestaram auxílio no diagnóstico de potenciais casos secundários de infeção provenientes de situações de proximidade entre indivíduos diagnosticados com COVID-19 e outros indivíduos cuja identidade não fosse ainda conhecida.[10] Desde a aplicação *StayAway Covid* em Portugal, à

[7] Joseph Tan, 2005, E-health Care Information Systems: An Introduction for Students and Professionals, Jossey Bass, pp. 40-44; 230-234;

[8] Cfr. European Comission (2019), Research and innovation in the field of ICT for health, wellbeing andageing, an overview: Directorate-General for Communications Networks, Content and Technology - Digital Society, Trust and Cybersecurity, disponível em https://ec.europa.eu/information_society/newsroom/image/document/2019-33/health_ageing_projects_list_2019_6BC92EFF-90F3-8A94-09FBFA3C4DFD150E_61321.pdf [acesso: 17.11.2024].

[9] Cfr. Organização Mundial da Saúde (2020, 11 de março), WHO Director-General's opening remarques at the media briefing on COVID-19, disponível em: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 [acesso: 18.11.2024].

[10] Joel A. Alves, 2021, StayAway Covid e Direitos Fundamentais in Desafios do Direito no séc. XXI: Diálogos Luso-Brasileiros, Governação e Covid-19, JusGov, pp. 53-58.

Corona-Warn-App na Alemanha, passando pela *TousAntiCovid* na França, as soluções digitais nacionais, a par das orientações da União, perpetuaram um acérrimo esforço no combate à crise pandémica através do método da rastreabilidade.

Neste seguimento, outros esforços foram ainda desenvolvidos pelas instituições europeias: implementou-se o *EU Digital COVID Certificate* [11] , destinado a promover uma mobilidade segura dentro da União, sem restrições excessivas; e o programa *SURE (Support to mitigate Unemployment Risks in an Emergency)* [12] orientado para a mitigação de crises laborais e para a preservação da coesão económico-social no condicionalismo pandémico. Deste modo, irrefragável é a ideia de que a crise sanitária em questão alterou a concepção de saúde europeia, ensinando lições aos Estados-Membros e promovendo a urgência de se repensar a forma como futuramente se enfrentará outras semelhantes adversidades.

Já no cenário pós-pandémico, a Comissão Europeia continuou a empreender esforços interoperáveis, designadamente através da proposta legislativa *European Health Data Space* (*EHDS*), projetada para a acessibilidade e partilha de dados eletrónicos que promovem a prestação de cuidados médicos e a investigação científica. Portanto, esta iniciativa, permite suprir as lacunas dos sistemas de saúde enfatizadas pela pandemia e promover a interoperabilidade no domínio *e-Health*. Consequentemente, apresenta-se como uma severa contribuição para a transformação digital da saúde da União, e, concomitantemente, antecipa respostas céleres e eficientes a futuras e eventuais emergências sanitárias.[13]

Efetivamente, a digitalização da saúde configurou-se como vital e determinante no combate à pandemia da COVID-19: fomentou a capacidade de resposta dos sistemas de saúde, permitiu o acesso remeto a cuidados médicos e dinamizou a gestão de dados relevantes em tempo real. Além do mais, o paradigma *e-Health* apresentou-se, uma vez mais, como um fenómeno pivô para o futuro, para a resiliência e para a subsistência dos sistemas de saúde europeus.

***e-Health*, cibersegurança e conformidade com o RGPD**

De facto, é indubitável que a interoperabilidade postula a articulação entre sistemas e bases de dados, possibilitando o acesso a dados de saúde e uma mudança nos padrões norteadores da investigação. Neste sentido, brotam preocupações de cibersegurança, até porque mais exigente do que a interoperabilidade no seio dos próprios Estados é a interoperabilidade no contexto da União. Consequentemente, cumpre evocar o

[11] Cfr. Comissão Europeia. (2021). EU Digital COVID Certificate, disponível em: EU Digital COVID Certificate - European Commission [acesso: 18.11.2024].
[12] Cfr. Comissão Europeia. (n.d.). SURE – Apoio para mitigar riscos de desemprego em situação de emergência, disponível em: SURE - European Commission [acesso: 18.11.2024].
[13] Cfr. European Health Data Space. (n.d.). *European Health Data Space: A European initiative for better health data management,* disponível em: https://www.european-health-data-space.com/ [acesso: 19.11.2024].

Regulamento Geral da Proteção de Dados (RGPD)[14] e o Regulamento 2018/1725[15], ambos propensos a assegurar que os dados fluam entre sistemas com respeito pela privacidade e pela segurança dos indivíduos. Note-se, porém, que este último é particularmente aplicável aos órgãos e instituições da União Europeia, ao passo que o RGPD aplica-se a todos os entes (públicos e privados) responsáveis pelo tratamento de dados pessoais com finalidades não domésticas.[16]

Não obstante a inovação e a evolução, é um facto que a transição digital também acarreta riscos e desafios. No caso das aplicações móveis de *contact tracing e mHealth*, por exemplo, estão em causa funcionalidades de geolocalização e de tratamento de dados pessoais, algo que pode vir a revelar-se intrusivo a nível dos direitos fundamentais e da cibersegurança. Neste seguimento, o Comité Europeu e a Comissão implementaram um conjunto de orientações em matéria de proteção de dados e de informação pautada pela sua sensibilidade. Neste sentido, exigiu-se uma definição exata do responsável pelo tratamento dos dados associados às supramencionadas aplicações, nos termos dos artigos 4º/7 e 5º/2 do RGPD; impôs-se uma precisão dos horizontes temporais orientados para a manutenção da informação recolhida; e salvaguardou-se a proteção dos inalienáveis direitos dos utilizadores enquanto titulares de dados pessoais, de acordo com o capítulo III do RGPD.[17]

Neste seguimento, é possível constatar que o domínio digital na saúde é indissociável do tratamento de dados, designadamente pessoais. Ora, nos termos do art. 4º/1 do RGPD, estes consistem na "informação relativa a uma pessoa singular identificada ou identificável". E partindo desta conceção geral, o quadro legislativo europeu em matéria de proteção de dados agrega ainda uma categoria de dados sensíveis, onde se inserem os dados relativos à saúde (art. 9º RGPD), ou seja, os "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular" – art. 4º/15 RGPD. Contudo, esta rigorosa proteção sofre algumas limitações à luz do art. 9º/2 RGPD, que estabelece exceções à regra gera de proibição do tratamento de dados sensíveis com carácter vinculativo e em articulação com o considerando 53 do mesmo diploma legal.[18]

Deste modo, excetua-se a proibição da gestão, recolha e análise de dados de saúde em diversas situações, nomeadamente quando o

[14] Cfr. Regulamento (UE) nº 2016/679, do PE e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[15] Cfr. Regulamento (UE) nº 2018/1725, do PE e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) nº 45/2001 e a Decisão nº 1247/2002/CE.

[16] Joana Covelo Abreu, 2020, A e-saúde (e-Health) no contexto da presente emergência pandémica – a proteção de dados pessoais e a interoperabilidade nas aplicações móveis de rastreamento de contactos (tópicas reflexões) in Manuela Martins, Eloy Rodrigues (Ed.), A Universidade do Minho em tempos de pandemia: Tomo III - Projeções, UMinho Editora, pp. 242-245

[17] Joel A. Alves, 2021, StayAway Covid e Direitos Fundamentais in Desafios do Direito no séc. XXI: Diálogos Luso-Brasileiros, Governação e Covid-19, JusGov, pp. 60-65.

[18] Tatiana Duarte, 2018, artigo 9º in Alexandre Sousa Pinheiro (ed.), Comentário ao Regime Geral de Proteção de Dados, Coimbra, Almedina, pp. 238-241.

titular dá o seu consentimento explícito para o tratamento ou quando os torna manifestamente públicos; quando os dados em questão revelam-se indispensáveis face a graves ameaças à saúde pública, incluindo catástrofes sanitárias ou crises médicas transfronteiriças; e quando o tratamento destes dados afigura-se crucial para a prossecução de finalidades estatísticas ou de investigação científica, priorizando-se sempre o interesse coletivo. Importa, porém, referir que o art. 9º/4 RGPD possibilita a alteração ou a adição de condições e limitações no que concerne ao tratamento de dados de saúde: em Portugal, este mecanismo materializa-se, essencialmente, na Lei nº 58/2019 de 8 de agosto[19], mais concretamente no seu art. 29º/1, onde é densificado o princípio da necessidade de reconhecer informação.

Em suma, perante a essência dos dados sujeitos a proteção reforçada (como é o caso dos dados relativos à saúde), realça-se a necessidade de promoção da literacia digital. Aqueles que recorrem a cuidados médicos devem estar cientes dos direitos e benefícios que lhes assistem no âmbito da articulação de sistemas, bem como dos possíveis malefícios no que concerne à cibersegurança. A participação dos cidadãos assume-se vital neste contexto, uma vez que estes devem juntar-se às devidas entidades públicas e privadas, nacionais e europeias, para a construção de uma interoperabilidade administrativa à luz do paradigma *e-Health*. Todavia, ambiciona-se uma cautelosa e responsável harmonização de sistemas, assente na fomentação do Mercado Único Digital e na proteção jusfundamental de dados pessoais a nível da União Europeia, balizada por padrões éticos de segurança e privacidade.[20]

A saúde transfronteiriça e a interoperabilidade dos sistemas de saúde dos Estados-Membros

A saúde transfronteiriça consiste no acesso a cuidados médicos em Estados-Membros da União Europeia distintos daquele em que o paciente está segurado. Abrange, portanto, a mobilidade dos doentes e o reembolso dos respetivos custos com base em normas europeias, designadamente o Regulamento 1408/71[21] e a Diretiva 2011/24/EU[22].

[19] Lei que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[20] Joana Covelo Abreu, 2019, Os Serviços Públicos Digitais na União Europeia: A interoperabilidade Administrativa e a Saúde Administrativa in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov, pp. 61-67.

[21] Cfr. Regulamento (CEE) n.º 1408/71 do Conselho de 14 de junho de 1971, relativo à aplicação dos regimes de segurança social aos trabalhadores assalariados, não assalariados e aos membros da sua família que se deslocam no interior da Comunidade.

[22] Cfr. Diretiva (UE) nº 2011/2014, do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativamente aos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

[23] Cfr. Comissão Europeia, 2018, Cuidados de Saúde Transfronteiriços, disponível em: https://op.europa.eu/pt/publication-detail/-/publication/45cdb89d-e952-11e8-b690-01aa75ed71a1 [acesso: 19.12.2024].

Assim sendo, é absolutamente essencial que os sistemas de informação de saúde dos Estados-Membros sejam pautados pela interoperabilidade, permitindo a troca de dados clínicos, bem como a partilha segura de prescrições eletrónicas. Além disso, a interoperabilidade administrativa revela-se imprescindível à cooperação entre as autoridades competentes para a concessão de autorizações e reembolsos, sem esquecer a monitorização dos cuidados administrados. Ora, nada disto seria possível sem o apoio do Mercado Único Digital responsável pela promoção da digitalização dos serviços de saúde, nomeadamente através da implementação de plataformas que facilitam o fluxo de dados e o desenvolvimento da saúde em linha.[23]

Concisamente, é correto afirmar que a saúde transfronteiriça aproveita a interoperabilidade de sistemas para incitar a integração operacional, beneficiando do MUD para uma maior digitalização e acessibilidade dos cuidados.

O caso Elchinov vs. NZOK (C-173/09)[24]

Este caso do Tribunal de Justiça da União Europeia aborda a recusa de uma autorização prévia para o acesso a tratamentos num Estado-Membro que não é o Estado de residência do doente, à luz do artigo 22.º do Regulamento 1408/71. Elchinov, um cidadão búlgaro diagnosticado com um tumor ocular maligno procurou realizar na Alemanha um tratamento especializado e indisponível na Bulgária que, no seu entender, seria menos invasivo do que a remoção cirúrgica do olho (alternativa apresentada pelas autoridades búlgaras).

Face à recusa da NZOK (caixa nacional de seguros de doença da Bulgária), Elchinov iniciou um processo judicial com a ambição de obter a cobertura das despesas: na primeira instância, o tribunal administrativo anulou a decisão da NZOK, considerando que estavam reunidas todas as condições para a concessão da autorização prévia. Posteriormente, inconformada, a NZOK interpôs recurso para o Supremo Tribunal Administrativo, que anulou a decisão do tribunal da primeira instância e submeteu o caso para reapreciação. No âmbito desta reapreciação, uma nova peritagem confirmou que, efetivamente, o tratamento administrado a Elchinov na Alemanha não era praticado na Bulgária. Neste seguimento, o tribunal administrativo suspendeu a instância e submeteu várias questões prejudiciais ao Tribunal de Justiça, de modo a obter esclarecimentos sobre a conformidade da recusa da concessão da referida autorização com o Direito da União Europeia.

Desde logo, o Tribunal de Justiça considerou a recusa da NZOK incompatível com as normas comunitárias, entendendo que a autorização só poderia ser recusada perante motivos imperiosos de ordem e saúde pública. Acrescentou ainda que a decisão sobre a autorização deve basear-se numa avaliação individual e objetiva, sustentada em elementos

[24] Cfr. Acórdão do Tribunal de Justiça (Grande Secção) de 5 de outubro de 2010: Georgi Ivanov Elchinov contra Natsionalna zdravnoosiguritelna kasa, disponível em: EUR-Lex - 62009CJ0173 - EN - EUR-Lex [acesso 19.12.2024].

médicos e científicos, pretendendo-se uma análise casuística. Além disso, compete ao tribunal nacional decidir sobre o reembolso das despesas, devendo o montante ser igual ao previsto na legislação do Estado-Membro onde os cuidados médicos foram prestados.

De facto, o impacto do caso Elchinov vs. NZOK na interoperabilidade administrativa dos Estados-Membros foi notório: protegeu-se o direito à saúde no âmbito da liberdade de circulação e harmonizaram-se regras no domínio da saúde transfronteiriça. Resta-nos concluir que, neste caso, as limitações administrativas e burocráticas da época evidenciaram a falta de coordenação entre os sistemas de saúde da União. Atualmente, com o desenvolvimento de mecanismos como a Diretiva 2011/24/EU e a ferramenta MyHealth@EU[25], verifica-se a simplificação da prestação de cuidados médicos transfronteiriços assentes numa capacidade de resposta mais eficiente, inovadora e modernizada.

Reflexões conclusivas

A transformação digital que assoberba a Europa potencia o desenvolvimento dos sistemas de saúde através da desmaterialização de processos, da otimização dos recursos disponíveis e da prestação de cuidados médicos ancorados em tecnologias emergentes. Por conseguinte, urge salientar o fenómeno da saúde em linha e a paulatina adesão dos Estados-Membros ao mesmo, por via do mecanismo da interoperabilidade administrativa. Afinal de contas, a coordenação dos Estados no domínio transfronteiriço exige sistemas interoperáveis, dinâmicos, integrados e capazes de responder às exigências contemporâneas.

Na qualidade de pedra angular da digitalização europeia, o Mercado Único Digital levou à superação de paradigmas obsoletos, desligados da automatização e da inovação tecnológica. Neste sentido, cumpre reforçar os seus contributos a nível do fluxo de dados na União e da criação de ferramentas hodiernas e cruciais para que os sistemas médicos prosperem.

Mas apesar do progresso, há desafios que persistem: o panorama europeu de interoperabilidade deve aprimorar os serviços de saúde digitais e, concomitantemente, assegurar os inalienáveis direitos dos cidadãos. Assim sendo, o desenvolvimento das políticas dos Estados-Membros no contexto *e-health* exige a compatibilidade dos seus quadros legais e a consequente harmonização de práticas administrativas.

Rafael Magalhães

Mestrando em Direito Administrativo

Escola de Direito da Universidade do Minho

[25] Infraestrutura digital responsável pela fomentação da interoperabilidade administrativa e da partilha de dados médicos entre os Estados-Membros, designadamente por via de prescrições e resumos clínicos eletrónicos.

Bibliografia

Anabela Susana de Sousa Gonçalves, 2019, Processing of personal data concerning health under the GDPR in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov.

Isa António, 2019, O impacto da tecnologia no setor da saúde e dos direitos fundamentais do doente, in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov.

Joana Covelo Abreu, 2017, Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions, UNIO – EU LAW Journal, vol. 3.

Joana Covelo Abreu, 2019, Os Serviços Públicos Digitais na União Europeia: A interoperabilidade Administrativa e a Saúde Administrativa in Maria Miguel Carvalho (ed.), Yearbook eTec, Health Law and Technology, Jusgov.

Joana Covelo Abreu, 2020, A e-saúde (e-Health) no contexto da presente emergência pandémica – a proteção de dados pessoais e a interoperabilidade nas aplicações móveis de rastreamento de contactos (tópicas reflexões) in Manuela Martins, Eloy Rodrigues (Ed.), A Universidade do Minho em tempos de pandemia: Tomo III - Projeções, UMinho Editora.

Joel A. Alves, 2021, StayAway Covid e Direitos Fundamentais in Desafios do Direito no séc. XXI: Diálogos Luso-Brasileiros, Governação e Covid-19, JusGov.

Joseph Tan, 2005, E-health Care Information Systems: An Introduction for Students and Professionals, Jossey Bass.

Tatiana Duarte, 2018, artigo 9º in Alexandre Sousa Pinheiro (ed.), Comentário ao Regime Geral de Proteção de Dados, Coimbra, Almedina.

Outras referências

Comissão Europeia, 2018, Cuidados de Saúde Transfronteiriços, disponível em: https://op.europa.eu/pt/publication-detail/-/publication/45cdb89d-e952-11e8-b690-01aa75ed71a1 [acesso: 19.12.2024].

Comissão Europeia. (2021). EU Digital COVID Certificate, disponível em: EU Digital COVID Certificate - European Commission [acesso: 18.11.2024].

Comissão Europeia. (n.d.). SURE – Apoio para mitigar riscos de desemprego em situação de emergência, disponível em: SURE - European Commission [acesso: 18.11.2024].

European Comission (2019), Research and innovation in the field of ICT for health, wellbeing andageing, an overview: Directorate-General for Communications Networks, Content and Technology - Digital Society, Trust and Cybersecurity, https://ec.europa.eu/information_society/newsroom/image/document/201933/health_ageing_projects_list_2019_6BC92EFF90F38A9409FBFA3C4DFD150E_61321.pdf [acesso: 17.11.2024].

European Health Data Space. (n.d.). *European Health Data Space: A European initiative for better health data management,* disponível em: https://www.european-health-data-space.com/ [acesso: 19.11.2024].

Organização Mundial da Saúde (2020, 11 de março), WHO Director-General's opening remarques at the media briefing on COVID-19, disponível em: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 [acesso: 18.11.2024].

Legislação

Decisão (UE) nº 2015/2240, do Parlamento Europeu e do Conselho, de 25 de novembro, responsável pela criação de um programa relacionado com soluções de interoperabilidade.

Diretiva (UE) nº 2011/2014, do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativamente aos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

Lei nº 58/2019 de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Regulamento (CEE) n.º 1408/71 do Conselho de 14 de junho de 1971, relativo à aplicação dos regimes de segurança social aos trabalhadores assalariados, não assalariados e aos membros da sua família que se deslocam no interior da Comunidade.

Regulamento (UE) nº 2016/679, do PE e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre

circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Regulamento (UE) nº 2018/1725, do PE e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) nº 45/2001 e a Decisão nº 1247/2002/CE.

Jurisprudência

Acórdão do Tribunal de Justiça (Grande Secção) de 5 de outubro de 2010: Georgi Ivanov Elchinov contra Natsionalna zdravnoosiguritelna kasa, disponível em: EUR-Lex - 62009CJ0173 - EN - EUR-Lex [acesso 19.12.2024].

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

Estarão os nossos dados a salvo no seu uso aplicado ao aperfeiçoamento de *OpenAI*?

Esta é uma das questões com que cada vez mais frequentemente nos confrontamos, especialmente numa era em que os nossos dados pessoais alimentam diretamente o desenvolvimento tecnológico, nomeadamente da Inteligência Artificial (doravante IA). Queremos fazer um uso da IA, mas temos alguns receios, um deles é o da exposição e partilha massiva dos nossos dados pessoais. A IA já não pertence apenas ao domínio teórico ou académico, hoje é parte integrante das nossas vidas quotidianas, seja pessoalmente ou profissionalmente.

Focando-nos na *OpenAI*[1], estes modelos avançados de IA generativa, como o *GPT*, são aperfeiçoados com enormes quantidades de dados extraídos de diversas fontes públicas e privadas. No entanto, esta prática, embora essencial para o desenvolvimento tecnológico, levanta questões críticas sobre segurança e privacidade. Será que os nossos dados estão efetivamente protegidos quando são utilizados para aperfeiçoar algoritmos como os da *OpenAI*?

Neste artigo, procurar-se-á determinar, sob uma perspetiva técnica e jurídica, os riscos, as medidas de proteção atualmente utilizadas e a conformidade destas práticas com a legislação, particularmente com o Regulamento Geral sobre a Proteção de Dados (doravante RGPD). O objetivo é fornecer uma análise que permita compreender se os mecanismos atuais são suficientes ou se a nossa privacidade enfrenta novos riscos, sabendo-se que "o acesso aos dados é diretamente proporcional ao incremento do perigo de intrusão na vida privada dos cidadãos, relativamente aos quais pode passar a ser facilmente reconstituído o seu percurso de vida, pelos traços que vão deixando inscritos no mundo digital"[2].

A *OpenAI*, tal como outras soluções na vanguarda tecnológica, necessita de um volume considerável de dados para garantir a eficácia

[1] Note-se que existem diferentes tipos de IA, com as suas especificidades, diferenças e semelhanças. Neste artigo, o foco é a *OpenAI*. A *OpenAI* distingue-se de outros modelos de IA devido à utilização massiva de redes neuronais generativas pré-treinadas em larga escala, nomeadamente modelos GPT (*Generative Pre-trained Transformer*), que utilizam o paradigma *Transformer*, baseado em mecanismos avançados de atenção (*attention mechanisms*). Enquanto outras plataformas, como a Google *DeepMind*, aplicam técnicas ou aplicações específicas (por exemplo, aprendizagem por reforço em contextos fechados ou modelos multimodais especializados), a OpenAI tem-se destacado pela ampla generalização das capacidades linguísticas dos seus modelos, aperfeiçoados com quantidades extremamente vastas e diversificadas de dados. Este tipo de abordagem exige uma atenção ainda maior às questões jurídicas e éticas relacionadas com a privacidade e segurança dos dados, justificando, assim, uma análise rigorosa e focada especificamente nesta entidade.

[2] Mafalda Barbosa. *Inteligência Artificial. Entre a Utopia e a Distopia, alguns problemas jurídicos*. 2.ª edição, Gestelegal, 2024, p.200

dos seus modelos, sendo "os sistemas de inteligência artificial, tanto melhores quanto mais dados nós tivermos e quanto mais dados diferentes e recolhidos para fins diferentes nós tivermos" [3]. Estes dados provêm frequentemente de fontes públicas como *websites*, artigos, livros, etc. O processo conhecido como *web scraping*, [4] embora tecnicamente legítimo em muitos contextos, é controverso sob o ponto de vista legal, especialmente quando implica dados pessoais. Este método envolve *scripts* ou *bots* programados para navegar automaticamente por páginas *web* e extrair informação estruturada ou semi-estruturada, que é posteriormente armazenada para diversos fins, tais como o aperfeiçoamento de algoritmos de IA. [5] Embora a utilização técnica do *web scraping* seja, em muitas circunstâncias, considerada legítima e mesmo necessária – por exemplo, quando utilizada para recolher dados públicos destinados a investigações científicas ou jornalísticas –, a sua aplicação torna-se controversa sob a perspetiva jurídica e ética, sobretudo quando os dados recolhidos são classificados como dados pessoais, nos termos do artigo 4.º, n.º 1, do RGPD. Ainda que os dados pessoais se encontrem disponíveis na Internet, isto não significa necessariamente que estejam isentos da proteção jurídica, nem que o seu tratamento automatizado seja livremente permitido[6].

Segundo o RGPD, qualquer tratamento de dados deve assentar numa base legal sólida, nas quais se destacam o consentimento explícito dos titulares, a execução de um contrato ou o interesse legítimo devidamente fundamentado. A dificuldade surge porque, frequentemente, a recolha massiva de dados da *web* ocorre sem que exista interação direta com os titulares desses dados, impossibilitando o consentimento direto ou informado. Do ponto de vista técnico, dados recolhidos sem consentimento direto requerem uma atenção especial quanto à sua anonimização ou pseudoanonimização. Contudo, a eficácia destas técnicas permanece em aberto, sobretudo devido à capacidade crescente dos algoritmos modernos em identificar novamente os dados supostamente anonimizados[7]. Para enfrentar os desafios da privacidade, a *OpenAI* recorre a técnicas avançadas como a anonimização, pseudoanonimização, *federated learning* e privacidade diferencial.

A anonimização, em teoria, protege totalmente a identidade dos utilizadores ao

[3] Lourenço Noronha dos Santos. "Inteligência Artificial e Privacidade", *In*, Manuel Lopes Rocha e Rui Soares Pereira (coord.), *Inteligência Artificial & Direito*. Almedina. 2020, p. 152.

[4] Entenda-se por uma recolha automatizada e massiva de dados presentes na Internet através de ferramentas informáticas específicas, de acordo com Ryan Mitchell. *Web Scraping with Python, collecting more data from the modern We*. 2018, O'Reilly Media, Inc., pp. 9-10

[5] De acordo com Vlad Krotov & Leiser Silva. "Legality and Ethics of Web Scraping". Twenty-fourth *Americas Conference on Information Syste*ms, 2018, p. 2

[6] Alessandro Mantelero. "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment". *Computer Law & Security Review*, Volume 34, Issue 4, 2018, p. 755-756.

[7] Mesmo quando os dados parecem seguros e anónimos, há uma crescente possibilidade técnica de, através de cruzamento de dados ou técnicas avançadas de aprendizagem automática, voltar a associar esses dados a indivíduos específicos, comprometendo assim a segurança e privacidade inicialmente pretendidas.

eliminar quaisquer referências que possam identificar diretamente os indivíduos. No entanto, com as técnicas sofisticadas atuais de *machine learning* e cruzamento de bases de dados, é possível identificar novamente indivíduos a partir de dados supostamente anonimizados[8].

A pseudoanonimização, por outro lado, oferece um nível intermediário de proteção, ao substituir identificadores diretos por identificadores artificiais. Esta técnica, embora aumente a segurança, não elimina por completo o risco de identificação indireta, especialmente em grandes volumes de dados.

O *federated learning* permite treinar modelos diretamente nos dispositivos dos utilizadores sem recolha centralizada de dados pessoais. Esta abordagem tem vindo a ganhar popularidade por reduzir significativamente o risco associado ao armazenamento central de dados sensíveis. Contudo, estas técnicas não são isentas de limitações. O *federated learning*, por exemplo, enfrenta problemas técnicos relacionados com a eficiência, segurança do dispositivo individual e escalabilidade.

Uma estratégia recomendável passa por combinar avanços técnicos recentes (como privacidade diferencial e *federated learning*) com uma atualização contínua e coordenada do enquadramento jurídico. Isto implica não só um reforço da cooperação interdisciplinar entre especialistas em tecnologia, juristas e decisores políticos, mas também uma abordagem preventiva e integrada da regulação.

A utilização de dados pessoais no aperfeiçoamento de IA levanta igualmente desafios éticos e jurídicos complexos. O RGPD obriga à transparência no tratamento dos dados pessoais, o que implica informar os titulares claramente sobre o destino e finalidade dos seus dados, um desafio particularmente complexo para a *OpenAI,* que frequentemente desconhecem os titulares individuais dos dados utilizados.

Adicionalmente, o exercício de direitos individuais como o "direito a ser esquecido" (artigo 17.º do RGPD), que prevê a eliminação total dos dados pessoais, torna-se problemático quando aplicado a modelos já implementados. Tecnicamente, eliminar informação específica de um modelo de IA pré-treinado não é apenas difícil, mas pode ser inviável, levantando sérias questões de conformidade legal. Por outro lado, coloca-se também a questão da responsabilidade legal por danos decorrentes do uso inadequado dos dados. Quem será responsável se um modelo causar prejuízos ou discriminar uma pessoa devido a dados enviesados ou incorretos utilizados no treino?

[8] Estudos recentes, como os de Rocher, Hendrickx e de Montjoye, demonstraram que a anonimização de dados pode ser revertida, através de técnicas modernas de cruzamento de bases de dados (*linkage attacks*), usando modelos avançados de aprendizagem automática. Este fenómeno põe em causa a eficácia das atuais metodologias de proteção, sugerindo que a anonimização clássica já não constitui uma salvaguarda robusta da privacidade. Luc Rocher, Julien Hendrickx & Yves-Alexandre Montjoye. "Estimating the success of re-identifications in incomplete datasets using generative models". *Nature Communications, 2019, 10*(1), 3069.

A atual legislação permanece pouco clara sobre quem recairá esta responsabilidade: a empresa que recolheu os dados, a entidade que desenvolveu o modelo ou quem aplica a tecnologia.

O panorama atual revela claramente que tanto o quadro jurídico, como os mecanismos técnicos existentes não estão totalmente alinhados com as exigências reais da privacidade e segurança. Olhando para o futuro, é essencial desenvolver soluções que assegurem simultaneamente a inovação tecnológica e o respeito pelos direitos fundamentais dos cidadãos.

Uma possível solução reside na criação de normas internacionais específicas para a utilização de dados pessoais para aperfeiçoamento de IA, acompanhadas por auditorias regulares e independentes. Adicionalmente, será importante melhorar as técnicas que permitam o controlo e remoção seletiva dos dados, adequando-se às exigências legais emergentes.

Apesar dos esforços significativos realizados pela *OpenAI* e outras entidades similares para proteger os dados pessoais, as limitações técnicas e jurídicas atuais mantêm a privacidade em risco. A conformidade total com o RGPD e a garantia absoluta de proteção da privacidade exigem uma cooperação mais estreita entre tecnologia e regulamentação, mas de acordo com Mafalda Barbosa "os algoritmos generativos colocam, do ponto de vista normativo, muitas dificuldades no que respeita à compatibilização com a intencionalidade do RGPD[9]. Enquanto não forem implementadas medidas técnicas e regulatórias mais robustas, é legítimo questionar se os nossos dados estarão verdadeiramente a salvo no contexto do aperfeiçoamento da IA pela *OpenAI*. A vigilância constante e uma regulação proativa são fundamentais para equilibrar a inovação tecnológica com os direitos fundamentais dos indivíduos, não perdendo o foco de um possível cenário futuro a que Arlindo Oliveira[10] nos alerta, uma realidade ainda mais complexa, no qual estes modelos generativos não só poderão utilizar os nossos dados pessoais, como eventualmente desenvolver formas avançadas de inteligência autónoma, tornando imperativa uma maior vigilância ética e jurídica.

Inês Freire dos Santos

Aluna de Doutoramento na Faculdade de Direito de Lisboa. Docente e Consultora em cibersegurança e IA.

[9] Mafalda Barbosa. *Inteligência Artificial. Entre a Utopia e a Distopia, alguns problemas jurídicos*. 2.º edição, Gestelegal, 2024, p.202

[10] Arlindo Oliveira. *Mentes Digitais, A Ciência Redefinindo a Humanidade*. Instituto Superior Técnico, 2018, pp.250-251.

Privacidade ou Conforto?

O mundo atual gira uma velocidade alucinante, ainda que, os dias mantenham as inalteráveis 24 horas.

O tema da proteção dos dados pessoais e a sua relevância no contexto contemporâneo nunca, como agora, teve tanto reflexo prático, no âmbito regulamentar e legislativo, no entanto, nunca foram aqueles tão devassados.

As empresas arriscam e continuam a aceder aos dados pessoais de cada um de nós, constituindo perfis, sem que tenhamos solicitado qualquer produto, ou sequer saibamos que, empresa é aquela que nos contacta, seja por email ou por telefone.

A última e mais importante devassa é sem dúvida os pagamentos eletrónicos.

Serão aqueles, definitivamente, mais confortáveis para todo e qualquer humano, no entanto no reverso da medalha está o "big brother" da monitorização de todos e quaisquer gastos que façamos, atendendo aos registos informáticos recolhidos, pelos vários intermediários existentes no mercado que, permitem os pagamentos pela via digital.

Estará a sociedade atual perante um novo paradigma? Entre o conforto e privacidade, escolhendo o segundo em detrimento do primeiro, sem informação suficiente ao nível, dos valores sacrificados, sobretudo no que, concerne ao registo total dos seus gastos e por consequência da tipologia de vida, permitindo com maior facilidade a definição de perfis e o contacto cada vez maior (e em violação dos dados) de empresas a oferecer produtos (sobretudo financeiros).

Ou pior, não terá, por consequência, e ao nível dos gastos em face dos rendimentos, repercussões na capacidade de crédito dos consumidores, vedando-lhes acesso aos empréstimos, até na compra de por exemplo: uma máquina de café a prestações?

Pedro João de Oliveira


AP
DPO
PORTUGAL