DPO mag

EDIÇÃO Nº 7
JUN/23

APDPO PORTUGAL

www.dpo-portugal.pt

DPO mag

EDIÇÃO Nº 7
JUN/23

APDPO PORTUGAL

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

Mensagem da Diretora

Inês Oliveira

Presidente da Direção da APDPO

Diretora da DPO Magazine

Bem-vindos à DPO Magazine n.º 7!

O primeiro semestre de 2023 foi marcado, permitam-me afirmar, pela divulgação da segunda ação coordenada de supervisão do Comité Europeu para a Proteção de Dados (CEPD) e das autoridades de proteção de dados europeias e pelo lançamento de um questionário dirigido aos encarregados de proteção de dados (EPD) nomeados e notificados junto das referidas autoridades, questionário esse sobre a sua designação e posição. O papel dos EPD está assim no centro da ação fiscalizadora da União Europeia para 2023, o que muito nos apraz.

Como explicou a nossa autoridade de controlo, a Comissão Nacional de Proteção de Dados (CNPD), enquanto intermediários entre as autoridades de proteção de dados, os indivíduos e as organizações, os EPD desempenham um papel essencial na garantia de uma melhor conformidade das organizações com a legislação de proteção de dados e na promoção de uma defesa efetiva dos direitos dos titulares dos dados. Não podíamos dizer melhor!

A referida ação coordenada de supervisão de 2023 conta com a participação de 26 autoridades de proteção de dados, nelas se incluindo a CNPD. O objetivo principal é conhecer melhor o papel desempenhado pelos EPD nas organizações, se detêm a posição exigida pelos artigos 37.º a 39.º do RGPD e se têm os recursos necessários para o desempenho das suas funções.

A ação é feita através de um questionário de matriz comum, de modo a que as respostas obtidas sejam analisadas de forma

coordenada e os resultados agregados e objeto de um relatório final do CEPD. Esta não será uma ação de investigação, uma vez que a CNPD pretende, antes de mais, ter um conhecimento mais aprofundado do papel dos EPD nas organizações, para que possa também encontrar formas de melhor apoiar o seu trabalho.

A nível nacional, a CNPD propôs-se contactar diretamente os EPD notificados por todas as organizações públicas e privadas para que participem voluntariamente nesta ação e respondam ao questionário.

A nós, APDPO, coube-nos apelar à participação de todos e cada um de nós, certos de que apenas uma grande participação possibilitaria o cumprimento dos objetivos.

Permitam-me dar um testemunho, enquanto profissional objeto deste questionário, que recebi e respondi prontamente, no dia 31 de março de 2023, ciente de que apenas uma grande participação nos dignificaria.

Chamado "Questionário sobre a designação e a posição dos encarregados de proteção de dados (EPD)" e integrando 39 perguntas, principiava com um pedido de informações gerais: Papel da organização (Responsável pelo tratamento; Subcontratante), Setor (Privado; Público) e Área de intervenção/âmbito de competência territorial (Nacional; Regional ou local).

O primeiro bloco de questões respeitava à designação, conhecimentos e experiência do Encarregado da Proteção de Dados (EPD), tendo perguntas como "Com base em que norma legal a organização designou um EPD?", "A pessoa designada desempenha também as funções de EPD para outras organizações do mesmo grupo empresarial (no caso de setor privado) ou para várias entidades públicas?", "O EPD é um elemento do pessoal da organização ou as tarefas são desempenhadas com base num contrato de prestação de serviços?", "Qual a duração da designação de EPD para o cargo?", "Quantos anos de experiência tem o EPD no domínio do direito e das práticas de proteção de dados?" e "Quantos anos de experiência relevante tem o EPD a trabalhar na área de negócio da organização?".

É neste primeiro bloco de questões que se começa a colocar *a mão na ferida*, perguntando-se o número de horas de trabalho por mês que o EPD despende nas funções de EPD, a experiência ou conhecimentos especializados do EPD, os requisitos para a designação e quantas horas de formação tem, anualmente, o EPD. Espero que a verdade das respostas alerte a CNPD para a realidade que a minha experiência me tem dado: EPD que trabalham poucas horas nessas funções, sem conhecimentos especializados, nomeações sem escrutínio das valências dos

profissionais e pouca (ou nenhuma) formação oferecida.

O segundo bloco de questões respeitava às funções e recursos do Encarregado da Proteção de Dados, integrando questões como "A direção da organização definiu claramente e forneceu-lhe uma descrição escrita das funções do encarregado da proteção de dados?", "A referida descrição escrita das funções do EPD foi comunicada ao pessoal da organização, ou as tarefas foram de outro modo notificadas ao pessoal?", "A descrição escrita das funções corresponde e abrange todas as tarefas efetivas do EPD na organização?", "Foram-lhe atribuídas funções adicionais, enquanto EPD, que não estejam previstas no RGPD?", "O EPD desempenha as suas funções a tempo inteiro?", "Quantos trabalhadores a tempo inteiro tem o EPD à sua disposição para o desempenho das suas funções?", "Considera que os recursos acima referidos são suficientes para desempenhar as funções de EPD?", "A organização atribuiu um orçamento ao EPD?" e "Quantos pedidos internos (formais ou informais) de aconselhamento sobre as obrigações decorrentes do regulamento sobre a proteção de dados recebe o EPD em média num mês?".

O terceiro bloco de questões visava o papel e a posição do Encarregado da Proteção de Dados e questionava-se: "Com que frequência o EPD está envolvido e/ou é consultado em questões relacionadas com a proteção de dados pessoais na organização?", "A consulta do EPD sobre questões relacionadas com a proteção de dados, por exemplo, violações de dados pessoais, é exigida pelos processos internos da organização?", "Em geral, o EPD tem acesso e dispõe de informações suficientes sobre questões relacionadas com a proteção de dados e as operações de tratamento de dados pessoais na organização, a fim de desempenhar as suas funções?", "Em geral, os pareceres e as posições do EPD são seguidos na organização?", "A organização deu-lhe instruções enquanto EPD sobre o exercício das suas funções?", "Alguma vez, na qualidade de EPD, foi penalizado pela organização pelo desempenho das suas funções?", "Através de que meio é que, na qualidade de EPD, esse reporte feito à organização?", "Os titulares dos dados têm a oportunidade de contactar o EPD em questões relacionadas com o tratamento dos seus dados pessoais ou com o exercício dos seus direitos?" e "Enquanto EPD, quantos pedidos de contacto (ou semelhantes) dos titulares dos dados recebe, em média, num mês?".

O último bloco de perguntas era atinente à orientação da Autoridade de Controlo e questionava "Na sua opinião, a autoridade de controlo da proteção de dados deve publicar os dados de contacto (endereço postal, um número de telefone específico

e/ou um endereço de correio eletrónico específico) dos EPDs, a fim de facilitar as obrigações de transparência?" e "Que tipo de orientações adicionais pretende que a sua organização receba das autoridades de controlo da proteção de dados, a fim de clarificar as funções e a posição do EPD?".

Enquanto profissional, foi imenso o gosto em colaborar preenchendo o questionário e proporcionando o conhecimento de uma realidade, que é a minha, esperando que os resultados espelhem a verdade de quem todos os dias se confronta com os problemas dos EPD.

Conteúdo

Sensibilização para situações de fraude

Fernanda Fragoso

EPD/DPO

SCML

A fraude é, genericamente, uma simulação da realidade endereçada às vítimas, através de e-mail, de sms ou por telefone, com o intuito, malicioso, do atacante (*hacker*) criar situações a partir das quais obtenha, normalmente, um ganho patrimonial por via da boa-fé das vítimas que são aliciadas a exporem informações pessoais e sigilosas.

Verifica-se, regularmente, que existe uma panóplia de ideias criativas de aliciamento através de mensagens fraudulentas direcionadas a atrair as vítimas. Estas mensagens transmitem sempre uma situação de urgência que leva as vítimas a agirem rapidamente, sob pressão, não ponderando, devidamente, o solicitado.

Através dos e-mails, mas também por sms, os utilizadores recebem muitas mensagens fraudulentas (conhecidas por *phishing*).

O *phishing* consiste num ataque informático pelo qual o atacante (*hacker*) simula ser uma pessoa ou uma entidade que, na realidade, não é.

Mesmo que o endereço do remetente seja válido isso não garante fiabilidade uma vez que o mesmo pode ser facilmente manipulável, é necessário avaliar se o conteúdo da mensagem lhe parece estranho procurando confirmá-lo por outros meios antes de dar a informação que estão a solicitar ou antes de abrir anexos ou clicar em *links* incorporados na mensagem.

São exemplos dessas mensagens os casos, denominados, de engenharia social:

- Mensagem sucinta de que ganhou um prémio solicitando-lhe,

para mais detalhes, que aceda ao *link* que lhe é fornecido;

- Notificação de um pagamento a fazer à autoridade tributária, cujo prazo está a terminar, dando a possibilidade de resolver o assunto através do *link* que lhe é fornecido;

- Alegados fornecedores enviam-lhe um novo IBAN, para pagamento dos serviços prestados.

Outros tipos de fraudes informáticas são por exemplo:

▪ As *deepfakes*, que constituem manipulação de imagens (mapeamento facial) ou de sons;

▪ O roubo de identidade (ex.: "Olá mãe", um tipo de fraude veiculada através do *WhatsApp*, em que os atacantes extorquiam dinheiro às vítimas). O crime de roubo de identidade é também usado para a obtenção de documentos falsos, por exemplo, para o *hacker* conseguir uma carta de condução ou obter um empréstimo bancário em nome da vítima;

▪ O *Network sniffing*, ou seja, a captura de pacotes de dados pessoais transmitidos na rede sem fios.

Focando-nos, em particular, nos casos de *phishing* que, diariamente, são noticiados pelos meios de comunicação social, verifica-se que a sensibilização para as situações de fraude passa, antes de mais, pela preocupação das empresas com a segurança da informação e comunicação de procedimentos internos que alertem para comportamentos seguros por parte utilizadores do sistema informático, em particular a especial atenção a ter com a adequada utilização do e-mail, bem como com a gestão das *passwords*.

No caderno de economia, do Jornal de Negócios *online*, de 22 de fevereiro, de 2023, lê-se*: "Fraude CEO" em crescimento em Portugal - no ano passado chegaram ao Ministério Público 23 denúncias de situações em que criminosos se fazem passar por fornecedores de uma empresa."*

De acordo com o relatado neste artigo, da autoria da jornalista Filomena Lança,

"São "técnicas de engenharia social" pelas quais se tenta levar uma empresa a efetuar pagamentos a terceiros que se fazem passar por autênticos fornecedores ou parceiros de negócios. Este tipo de situações são conhecidas na gíria policial como "CEO fraud", ou "business email compromise" e têm vindo a crescer em Portugal, de acordo com a Procuradoria-Geral da República."

A revista Visão *online*, no caderno SOCIEDADE, de 17.02.2021, publicou um artigo denominado "Os novos tipos de fraude nascidos com a pandemia" que, sumariamente, designou por "Corona-phishing".

De acordo com este artigo:

"Desde o início da pandemia foram também detetados muitos falsos negócios, que oferecem produtos

que não existem em sites, redes sociais, emails e ligações por telefone com o intuito de obter os dados bancários das vítimas – e até a OMS se viu obrigada a avisar que havia quem se andasse a passar por representantes da organização para obter doações falsas e roubar dados pessoais. Mas se, num primeiro momento, esse "phishing" se concentrava em falsas campanhas de caridade e na suposta venda de produtos muito procurados – como máscaras, álcool gel e desinfetantes – agora o tipo de golpe é bem mais sofisticado.

Por exemplo, na Argentina houve até bancos que tiveram de encerrar os seus perfis nas redes sociais desde que se soube que algumas informações ali partilhadas tinham permitido esvaziar as contas de alguns clientes. O que os criminosos fizeram foi contactar as pessoas que usaram a rede para expor um problema com a sua conta, dada a impossibilidade de atendimento pessoal nas agências bancárias – havia meses fechadas ao público. Apresentando-se como funcionários do banco conseguiram obter os detalhes da conta da vítima e, antes da esvaziaram, pediram um empréstimo. Ou seja, as vítimas não só perderam o dinheiro como ficaram endividadas.

A FTC (Federal Trade Commission) americana deu ainda conta de outra forma de fraude: pessoas que ligam para as "potenciais" vítimas a comunicar-lhes que estiveram com alguém que testou positivo à Covid-19. Recomendam que façam o teste o mais rápido possível e indicam o lugar onde o podem fazer. Depois, informam que, para receber o resultado mais depressa, será necessário fornecer logo, e antes de mais, o número do cartão de crédito, para cobrir os custos de envio."

O *phishing* foi a tipologia de crime mais reportada em 2022 ao Gabinete de Cibercrime. No ano passado verificou-se um aumento de 114,37% de casos de face a 2021. De 167 casos reportados ao MP em 2021, para 358 casos reportados em 2022.

Os alertas de fraude para a receção de chamadas telefónicas são, também, da maior importância, no combate a situações de fraude (ex.: contactos de falsos fornecedores da empresa).

Com efeito, a componente humana (dirigentes; colaboradores; fornecedores) de uma empresa constitui um dos principais riscos de segurança da informação, uma vez que as ações maliciosas ou mesmo negligentes, por parte dos utilizadores podem expor as vulnerabilidades e as defesas da empresa a ameaças permanentes, por vezes difíceis de detetar.

Os *hackers* andam muito ativos em ações de sequestro de informações e, particularmente, de dados pessoais.

Fraudes sempre existiram, mas a sofisticação dos meios atuais, quer por via da internet, quer pela maior

facilidade de comunicação telefónica ou por sms, trouxeram um mundo novo nesta área da criminalidade: os ciberataques. Releva, ainda o facto, deste crime poder ter origem a grande distância do destino visado pelo *hacker*, atacando uma área geográfica que por via da globalização, poderá ser em qualquer parte do mundo.

As empresas / instituições devem adotar os meios adequados, através da implementação de medidas técnicas e organizativas, que lhes garantam uma diminuição considerável do eventual risco de exposição da informação que tratam.

Uma das formas mais imediatas de minimizar este risco é através da dupla certificação de acesso, pela qual se consegue uma maior autenticidade na identidade dos utilizadores.

Esta medida técnica assume especial relevância nas situações laborais em regime de teletrabalho!

A *dark web* definida como uma parte da internet acessível apenas por meio de *software* especial é, na sua essência, um supermercado de dados! Com efeito, os atacantes podem adquirir dados na *dark web* para os utilizar numa atividade criminosa, por exemplo, de acesso a contas alheias.

Com efeito, mais de 80% dos atacantes utilizam *passwords* furtadas. Muitas pessoas continuam a ter apenas uma *password* para acesso a diferentes sites e, cumulativamente, algumas utilizam *passwords* básicas como 123456. Este tipo de negligencia facilita os atacantes a fazerem *login* em vários sites, com as mesmas credenciais.

O *malware* propaga-se através de programas ou de código maliciosos criados para invadir, danificar ou incapacitar computadores e outros dispositivos, sistemas ou redes, ou até para furtar, encriptar ou apagar dados.

O princípio da segurança do tratamento de dados pessoais, contemplado no artigo 32º, e no considerando 83, do RGPD, convoca a aplicação de medidas técnicas e organizativas adequadas para a segurança da informação. Concretizando, essas medidas podem ser:

- atualizações regulares do sistema operativo e de aplicações;
- implementação de políticas de segurança pelos postos de trabalho, designadamente:
- definição de procedimentos para os pedidos de acesso remoto à rede informática da empresa;
- definição de procedimentos para a dupla certificação no acesso aos sistemas da empresa;
- instalação de *software* de proteção da caixa do correio, através do qual há uma filtragem das mensagens duvidosas que ficam retidas em quarentena. Se o destinatário verificar que a

mensagem é legítima pode desbloqueá-la e enviá-la para a sua caixa do correio;

- proibição aos utilizadores de dispositivos que geram redes sem fios, como por exemplo os *routers*, uma vez que os mesmos podem expor vulnerabilidades da empresa e serem uma porta de entrada para intrusos;
- é da enorme importância para a segurança da informação haver uma consciente gestão das *passwords* por parte de cada utilizador, como por exemplo:
- escolher uma *password* para o posto de trabalho que não utilize noutros acessos à internet, especialmente nos acessos pessoais;
- memorizar as *passwords* e não as deixar escritas em locais visíveis;
- alterar, regularmente, as *passwords*;
- utilizar passwords seguras, mas fáceis de memorizar;
- nunca partilhar a *password* com ninguém;
- a implementação de controlos gerais:
- processo de gestão de utilizadores que assegura que os colaboradores possuem uma conta individual e não genérica;
- implementar um *software* de gestão de utilizadores;
- é fundamental o cancelamento dos acessos de colaboradores que já cessaram o seu vínculo profissional na empresa;
- a implementação de controlos aplicacionais:
- gestão de perfis no acesso à informação: perfis distintos na aplicação que assegurem que cada trabalhador só tem permissões de acesso à informação para as funções necessárias ao desempenho das tarefas que lhe estão atribuídas;
- os utilizadores só devem aceder aos processos dos seus utentes cuja informação têm de conhecer.

Constituem requisitos de privacidade e de segurança da informação da empresa:

- As Políticas de Privacidade e de Tratamento de Dados Pessoais;
- As Políticas de Segurança da Informação;
- Os Procedimentos e os Regulamentos internos.

As medidas técnicas e organizativas de segurança de informação não asseguram, isoladamente, grande eficácia no combate aos ataques informáticos. Para haver um nível de robustez adequado, designadamente, em matéria de segurança do tratamento dos dados pessoais, é absolutamente necessário o recurso a várias metodologias em simultâneo.

Numa abordagem de resistência aos ciberataques a segurança deverá ser efetuada por camadas, bloqueando os métodos de ataque mais simples e evoluir no combate aos métodos mais sofisticados.

Por exemplo, a utilização de um *firewall* avançado, a autenticação multifator, as ferramentas de deteção de automação, as verificações de transações, que conjuntamente podem contribuir para construir camadas de segurança (nas redes e nos sistemas informáticos) que impeçam as tentativas de fraude. Quantos mais obstáculos os *hackers* encontrarem, mais dificuldades terão na obtenção de sucesso da sua atividade criminosa.

A Comissão Nacional de Proteção de Dados – CNPD publicou, em 10 de janeiro de 2023, a Diretriz/2023/1, cujo teor recomenda, ao responsável pelo tratamento e, com as devidas adaptações, ao subcontratante, a adoção de medidas de segurança no tratamento de dados pessoais em cumprimento do disposto no artigo 32º, nºs 1 e 2, do RGPD.

Contudo, embora a Diretriz/2023/1, da CNPD não o mencione, é necessário continuar a avaliar o nível do risco, através da elaboração da avaliação do impacto sobre a proteção de dados – AIPD, constante no artigo 35º, do RGPD, designadamente nos casos exemplificados no nº3 do referido artigo.

Em 14 de dezembro de 2022, foi publicada a Diretiva (EU) 2022/2555, do Parlamento Europeu e do Conselho, (NIS2) que estabelece as medidas de gestão de riscos de cibersegurança e as obrigações de informação em todos os setores que se enquadram no seu âmbito de aplicação – energia; transportes; saúde; infraestruturas digitais.

O prazo de transposição por parte dos Estados Membros termina a 17 outubro de 2024.

A Diretiva NIS2 revoga a Diretiva (EU) 2016/1148 (SRI 2), que consagra o regime jurídico da segurança do ciberespaço – por via de medidas destinadas à segurança das redes e dos sistemas de informação. Esta Diretiva foi transposta para o direito nacional pela Lei nº 46/2018, de 13 de agosto.

Outro importante instrumento de combate à fraude, em particular nos meios de pagamento, é a Diretiva (UE) 2019/713 que atualiza "*as regras em vigor em matéria de luta contra a fraude e de fabrico de meios de pagamento que não em numerário (cartões de crédito, compras em linha, etc.), a fim de assegurar a existência de um quadro jurídico claro, sólido e tecnologicamente neutro*".

A referida Diretiva vem ainda facilitar a investigação e a ação penal e prevê ações para aumentar a sensibilização do público para as técnicas fraudulentas, como a mistificação da interface ('*phishing*') ou a clonagem ('*skimming*').

Entende-se, na linha de pensamento de outros especialistas em proteção de dados pessoais, não haver um dever do EPD/DPO comunicar, junto da autoridade nacional, situações de deteção de fraude. Sem embargo das funções de aconselhamento do EPD/DPO, contempladas no artigo 39º, nº1, alínea a), do RGPD, designadamente para com o responsável pelo tratamento - RT, esse dever formal de reporte à CNPD, em situações de fraude, é competência do responsável pelo tratamento.

As funções do EPD/DPO são, fundamentalmente, as de garante da conformidade com o RGPD!

JOGOS SANTACASA
uma boa aposta

TALENTO

O DESPORTO TEM TODO O NOSSO APOIO.

Ser o maior patrocinador do desporto em Portugal é apoiar o **TALENTO** e os grandes eventos desportivos nacionais. É promover a conciliação do desporto com a vida académica. É ir mais além em cada modalidade patrocinada, apoiar as nossas seleções, fazer crescer as competições nacionais, valorizar o desporto feminino e desenvolver o desporto adaptado. É fazer do desporto um fator de integração social.
Porque, para os Jogos Santa Casa, o Desporto é para Todos.

Apoiamos
Comités Olímpico e Paralímpico
19 Federações Desportivas
+ de 100 Seleções Nacionais

Atribuímos
422 Bolsas de Educação,
no valor de + de 1,2 milhões de euros

www.jogossantacasa.pt

Atletas (da esquerda para a direita): Rita Lagartinho, Tomás Appleton, Eduardo Picoito, Dinis Costa, Rita Vieira, Ana Oliveira, Diogo Ganchinho, Diogo Chen, Márcia Costa, Melanie Santos, José Ramalho, Rui Silva, David Grachat, Catarina Monteiro, David Rosa, Teresa Bonvalot, Patrícia Sampaio.

Anonimização e "Pseudonimização"

Vitorino Gouveia

DPO Externo e Especialista em Segurança da Informação e Proteção de Dados

xis-group.com

A inclusão no Regulamento Geral sobre a Proteção de Dados (RGPD) da "pseudonimização" como medida para a proteção de dados é novidade face à diretiva europeia anterior. Senão vejamos, no RGPD a palavra (ou o conceito) "pseudonimização" é referida 15 vezes no RGPD, enquanto na diretiva anterior não constava.

A rápida evolução tecnológica dos últimos 10 anos exponenciou a necessidade de interação e transferência de dados entre aplicações e sistemas conectados em nuvem (incluindo para países fora da União Europeia). Os tratamentos de dados, incluindo as características, comportamentos e preferências pessoais, consubstanciada na definição de perfis, a computação em larga escala usando algoritmos de inteligência artificial e aprendizagem profunda (deep learning) suportam novos modelos de negócio, com benefícios para as organizações, mas, por outro lado, poderão impactar nos direitos e liberdades dos titulares dos dados, em especial na sua privacidade.

A utilização da anonimização e da pseudonimização são medidas que as organizações têm ao seu dispor (desde a conceção dos tratamentos e por defeito) para a proteção dos dados pessoais dos seus utilizadores, clientes, colaboradores ou outros titulares. Quando corretamente aplicadas, mitigam (ou evitam no caso da anonimização) o risco de exposição da privacidade dos titulares de dados pessoais quer a terceiros (que não tenham "necessidade de saber") quer para outras finalidades de tratamento, sem comprometer a operação e os negócios.

Em jeito de perguntas, vamos entrar no tema do título:

Em que consiste a anonimização e a pseudonimização dos dados? Quais as diferenças?

A principal diferença entre dados anonimizados e dados pseudonimizados é que os primeiros (os anonimizados) deixam de ser dados pessoais pois não permitem a reidentificação de pessoas singulares, e os segundos (pseudonimizados) continuam a sê-los, nos termos do RGPD.

Conforme previsto no RGPD, os dados pseudonimizados poderão ser reidentificáveis usando "informação adicional", mantida separadamente dos dados pseudonimizados e sujeitos a medidas técnicas e organizativas para garantir que somente nas situações previstas será possível a reidentificação.

Uma deficiente anonimização é aquela que permite a reidentificação das pessoas singulares. Uma das vulnerabilidades exploradas é a reidentificação pela utilização de identificadores indiretos mantidos nos registos pós-anonimização, p.ex. data de nascimento, código postal, género.

Outra falha recorrente na anonimização é a utilização de algoritmos de encriptação de dados para "supostamente" anonimizar dados pessoais. Uma vez identificada a chave para o algoritmo usado, os dados são passíveis de serem reidentificados. Mesmo quando a chave para a desencriptação não for conhecida, não é garantido que a reidentificação não possa ser possível num futuro mais ou menos próximo: vai depender da robustez do algoritmo, da utilização ou não de "sal" (conjunto de caracteres aleatórios) nas funções de geração dos hashs de encriptação e, da capacidade da computação disponível para reverter a encriptação por tentativa/erro (prevê-se que a utilização de computação quântica poderá reduzir exponencialmente o tempo necessário para quebrar os códigos criptográficos).

Uma boa prática passa por apagar definitivamente os dados que permitam a reidentificação ou substituí-los por carateres sem qualquer ligação algorítmica com o original.

A encriptação não é uma técnica de anonimização, mas poderá ser uma poderosa ferramenta para a pseudonimização. Protege a confidencialidade dos dados aplicando um algoritmo de cifra (simétrico ou assimétrico) onde a(s) chaves são conhecidas. As chaves poderão ser consideradas "informação adicional" que permite a reidentificação das pessoas singulares.

Qual o interesse / vantagem de aplicação destas ferramentas/ técnicas aos dados pessoais?

Como referido anteriormente são duas técnicas muito úteis para a

proteção de dados pessoais e devem ser usadas desde a conceção e por defeito.

A anonimização é uma alternativa muito útil à eliminação de registos contendo dados pessoais. Poderá ser usada, p.ex. na execução de um pedido de exercício do "direito ao apagamento" de dados pessoais ou, findo o prazo de conservação dos dados pessoais. A utilização de anonimização permite evitar falhas de integridade referencial nas bases de dados existentes, pela eliminação de registos contendo dados pessoais (i.e. mantendo referências nulas ou inexistentes para os registos eliminados, provocando erros ou falhas no normal funcionamento do sistema). É igualmente uma boa medida a usar na preparação e partilha de dados para a realização de operações nas quais não sejam necessários dados identificáveis, p.ex. tratamento estatístico, análise de dados e comportamentos de uma população para a tomada de decisão.

A pseudonimização é uma poderosa medida para a proteção de dados pessoais que pode ser aplicada "desde a conceção" aos repositórios de dados. Neste caso, as estruturas de dados são desenhadas para separar tipologias de dados pessoais e controlar a agregação ("por defeito"), apenas a perfis de utilizadores ou agentes autónomos autorizados. Por exemplo, na conceção de uma base de dados de registos clínicos de pacientes, os dados de identificação, os dados de contacto e os dados de saúde poderão ser armazenados em três tabelas ou estruturas de dados distintas, sendo os identificadores (que ligam os dados à identificação dos titulares) pseudonimizados. Assim, garante-se que a identificação dos titulares ocorrerá somente na medida da "necessidade de saber" exclusivamente aos utilizadores com autorização para tratar os dados clínicos, ou para tratar os dados pessoais de contacto. Neste caso, os registos cronológicos de acessos para auditoria (conforme previsto no princípio da "responsabilidade") são igualmente facilitados.

A utilização de pseudonimização permite mitigar o risco de falha na proteção de dados pessoais em atividades que envolvam por exemplo, a interação aplicacional, definição de perfis, marketing direto ou na partilha de dados com entidades externas no âmbito das atividades de tratamento de dados pessoais definidas.

Quais as pessoas / departamentos / entidades que as devem aplicar?

Estas medidas poderão ser aplicadas tanto pelas entidades Responsáveis pelo Tratamento como pelos seus subcontratantes (neste caso seguindo as instruções do Responsável pelo Tratamento).

A aplicação de anonimização ou pseudonimização nas atividades de tratamento de dados pessoais, deverá estar definida no inventário

das atividades de tratamento. O procedimento a aplicar, incluindo o algoritmo/ferramenta deve ser conhecido pelos intervenientes e validado pelo Encarregado de Proteção de Dados.

A sua aplicação prática poderá ser realizada por qualquer interveniente autorizado, nos processos de tratamento de dados pessoais. Poderá igualmente ser aplicada automaticamente por um algoritmo (e sem intervenção humana) para conjuntos de registos que satisfaçam as regras de elegibilidade definidas, p.ex. anonimização dos dados findo o prazo de conservação ou pseudonimização dos registos de dados, antes da transferência internacional para um subcontratante no âmbito de uma relação contratual.

Que riscos e quais as limitações que poderão existir com a aplicação de anonimização e pseudonimização?

A incorreta aplicação da anonimização poderá levar à reidentificação posterior dos dados com impacto na privacidade dos titulares ou à perda irreparável de dados, pela aplicação de anonimização errónea ou excessiva de dados, provocando a indisponibilidade dos dados incorretamente anonimizados quando necessário.

Os algoritmos de anonimização devem ser adequadamente testados por forma a garantir a sua eficácia (i.e. que exclusivamente os registos elegíveis para serem anonimizados assim o são), que a integridade dos dados que não são alvo da anonimização é salvaguardada e a garantia de não reidentificação dos titulares de dados.

Na pseudonimização é fundamental que as chaves de cifra, tabelas de afetação ou outras "informações adicionais" que permitem reverter a identificação dos titulares sejam mantidas separadas e armazenadas de forma segura, por forma a evitar uma reidentificação não autorizada ou ilegítima dos registos que origine uma violação de dados pessoais, nos termos do RGPD.

Importante realçar também que, uma utilização desproporcional da encriptação como via para a pseudonimização, poderá provocar degradação na performance ou na capacidade dos recursos dos sistemas de suporte. Estes algoritmos (e as operações de encriptação e desencriptação de grandes quantidades de registos) consomem muito mais recursos de processamento e armazenamento quando comparado com a utilização dos dados no seu formato original.

Pela minha experiência enquanto DPO externo e consultor nas áreas de segurança da informação e proteção de dados, verifico que a aplicação de anonimização ou pseudonimização de dados em sistemas informáticos já existentes é um grande desafio para as

organizações e poderá inclusive não ser tecnicamente exequível. Alguns exemplos de condicionantes comuns são: as limitações técnicas e pouca flexibilidade para evolução das estruturas de dados, dos pacotes de software "fechados" e das APIs existentes bem como a proliferação de dados pessoais em diferentes repositórios (incluindo o suporte físico em papel ou nos backups armazenados) que condicionam a sua aplicação e poderão ser fontes para a reidentificação dos dados no futuro.

Já ouviu falar no ChatGPT?

Martha Leal

Advogada

JPLeal

É bem provável que você já tenha ouvido falar do ChatGPT.

E talvez você já tenha até mesmo interagido com a tecnologia e se surpreendido com a sua capacidade de compreensão às perguntas formuladas e a adequação das suas respostas.

Entretanto, independentemente do nível de conhecimento que você detenha, importante tecermos algumas considerações básicas acerca do assunto e de seus prováveis impactos para uma melhor compreensão do assunto.

Optamos por iniciar decifrando sobre o que trata essa tecnologia e qual o seu diferencial sobre as outras, possibilitando assim, realizarmos inflexões acerca da sua própria evolução e prognosticar um futuro em que inevitavelmente estaremos cada vez mais conectados ao avanço da inteligência artificial.

O ChatGPT é um modelo de linguagem capaz de predizer respostas em um ambiente de bate papo. Ele foi adaptado através de um modelo já existente, o GPT-3.5, para se comportar como se fosse um humano.

Para melhor compreensão, importante entendermos o que significa a sigla GPT para "Generative Pretrained Transformer". Trata-se de um modelo de linguagem que possibilita que um texto faça sentido para a compreensão humana. Esse modelo de inteligência artificial é baseado no método de redes neurais, caracterizado como um processo de "machine learning", chamado aprendizado profundo e que usa neurônios intraconectados em uma

estrutura em camadas, similar ao cérebro humano.

A OpenAI, laboratório de pesquisa de inteligência artificial que criou o ChatGPT, apresentou a primeira versão da tecnologia em 2018, mas foi apenas em 2020 que a tecnologia despertou a atenção com a sua terceira versão, o GPT-3, que contava com um modelo treinado com 175 bilhões de parâmetros e uma base muito mais robusta de textos.

Agora, estamos na quinta versão e a tecnologia apresenta técnicas aprimoradas e que permitem receber instruções mais complexas e consequentemente gerando respostas muito mais coerentes.

Acresça-se a isso o fato de que a versão GPT-3.5 foi treinada com uma base gigante de textos disponíveis na web, incluindo posts em redes sociais e conteúdos disponibilizados nos meios de comunicação.

O ChatGPT apreende com os feedbacks dos usuários fazendo com que as suas respostas sejam cada vez mais coerentes e rápidas, o que nos permite ter expectativas do aprimoramento constante da tecnologia a partir das interações com os usuários.

Selecionamos para fins de melhor entendimento do funcionamento e o potencial da ferramenta, a resposta fornecida pelo próprio ChatGPT a uma de nossas interações, ao questionarmos como se dá o seu funcionamento. Eis a resposta:

“ O ChatGPT é um modelo de linguagem que foi treinado para gerar respostas a perguntas e comandos de usuários de maneira que pareça que está conversando com um ser humano. Ele foi criado com base em uma grande quantidade de dados de texto e foi treinado usando técnicas de aprendizado de máquina para apreender a produzir respostas apropriadas e coerentes a diferentes tipos de entrada. Em resumo, o ChatGPT é uma ferramenta de linguagem que foi projetada para simular uma conversa humana de maneira natural e coerente. Ele pode ser usado em vários contextos para fornecer respostas e interações automatizadas com usuários.”

A amostra acima ilustra que um simples comando do usuário para que a tecnologia descreva resumidamente o seu comportamento já fornece subsídios da sua habilidade em parecer humano, provendo informações e aconselhamentos ao que lhe é demandado.

E não há dúvidas de que este é apenas o começo de uma disruptiva forma de utilização da IA, onde ao buscarmos informações em formato de perguntas e respostas, sobre os mais diversos temas, somos abastecidos com conhecimento, referências e a depender da formulação da interação, com aconselhamentos.

Estabelece-se assim, uma nova forma de buscador de pesquisa,

eficiente e amigável na experiência com o usuário.

Entretanto, como qualquer modelo de linguagem abastecido por um grande volume de dados, o ChatGPT apresenta riscos e impactos associados ao seu uso, tais como, preconceitos e discriminação, entre outros.

Selecionamos alguns riscos da tecnologia que merecem destaque, senão vejamos:

A ferramenta é capaz de servir como um ótimo propósito educacional, auxiliando na resolução de problemas e aprendizados de novos conhecimentos, mas requer seja utilizada com responsabilidade. Pois, apesar de alguns resultados impressionarem pelo grau de coerência e robustez, não significa que as informações fornecidas sempre sejam verdadeiras ou que sequer façam sentido, ficando ao encargo do usuário verificar a veracidade de qualquer informação fornecida pelo modelo de linguagem, mesmo que o linguajar empregado demonstre plena convicção e propriedade sobre o assunto questionado.

Outro ponto relevante é a capacidade do ChatGPT vir a se tornar um grande buscador. Inquestionável que com todo o seu potencial, tem condições de competir ou complementar ferramentas na web como o Google.

De fato, já existem rumores que o modelo pode ser incorporado na ferramenta Bing da Microsoft e a OpenAI.

Com o cenário atual, é possível conjecturarmos que é provável que modelos de linguagem como estes que estão sendo criados e aprimorados atualmente, não venham a substituir, mas sim, complementar mecanismos de busca, por conta de seus diferentes propósitos. Embora o ChatGPT ofereça uma melhor resposta à pergunta do usuário, ainda não é possível usá-lo para navegar na web.

No campo da saúde, estudo recentemente publicado pela Drexel University (EUA), demonstrou que o ChatGPT-3 tem capacidade de fornecer subsídios que indiquem o começo de uma demência com 80% de acurácia, a partir da linguagem natural do usuário que interage com a ferramenta. Conforme palavras do autor da pesquisa publicada no “PLOS Digital Health”, Felix Agbavor, a análise da linguagem que o modelo de IA em questão faz, o torna um candidato promissor para reconhecer alterações sutis no discurso que podem indicar o princípio de um quadro de demência.

Impõe-se, portanto, o reconhecimento do potencial da tecnologia, os seus benefícios e os riscos decorrentes do seu mau uso.

Na busca de uma IA ética e responsável, é indispensável garantir que a base de treinamento da tecnologia seja diversa e equilibrada, reduzindo o risco de

reproduzir preconceitos e discriminação.

Partindo do reconhecimento que o ChatGPT é treinado por uma ampla base de dados, corolário lógico é a conclusão de que, se porventura, essa base estiver contaminada com viés discriminatórios, esses padrões consequentemente serão refletidos nas respostas geradas pelo modelo.

Nesse sentido, reconhecemos a magnitude da tecnologia, o potencial incalculável de seus benefícios, bem como, os desafios impostos, naturais a todo e qualquer modelo disruptivo, e que confirma a importância de desenvolvermos e fortalecermos regulações sobre a inteligência artificial, a exemplo da Proposta de Regulação da Inteligência Artificial da União Europeia, IA ACT e a Proposta de Regulação da Inteligência Artificial no Brasil, apresentada no final do ano ao senado Federal.

As mesas de restaurantes podem estar abrangidas por câmaras de um sistema de videovigilância?

Jorge Martinez Batalha

Mário Peixinho

Segurança e Privacidade 5.0

Antes de dar resposta à pergunta principal podem ser levantadas, entre outras, as seguintes questões:

1. Existirá necessidade, ou interesse legítimo do proprietário de um restaurante, de registar, num sistema de videovigilância, cuja finalidade seja a proteção de pessoas e bens, de que forma os clientes comem, por exemplo, se com a boca mais aberta ou mais fechada? Ou se sorriem muito, ou pouco, ao longo da refeição?

2. Existirá necessidade, ou interesse legítimo do proprietário de um restaurante, de registar, num sistema de videovigilância, cuja finalidade seja a proteção de pessoas e bens, a quantidade de copos de vinho (ou outros líquidos alcoólicos) que cada um dos clientes ingeriu?

3. Existirá necessidade, ou interesse legítimo do proprietário de um restaurante, de registar, num sistema de videovigilância, cuja finalidade seja a proteção de pessoas e bens, ao lado de quem cada uma das pessoas se sentou à mesa, quais os sinais/indícios de orientação sexual dos clientes, as manifestações de afeto que os clientes tiveram ou quais as crianças que estavam à mesa e também como estas se comportaram?

Na verdade, um sistema de videovigilância que abranja as mesas de um restaurante, por mais simples que este seja, pode recolher e gravar as imagens de todos os

aspetos indicados nas questões anteriores. E muito mais...

O Regulamento Geral sobre a Proteção de Dados (RGPD) não fala especificamente sobre videovigilância. Partindo deste regulamento, cada Estado-Membro da União Europeia produziu legislação complementar, incluindo o estabelecimento de alguns limites e regras em matéria de videovigilância.

No entanto, em Portugal, apesar do disposto na legislação complementar ao RGPD, em especial quanto ao estabelecido no artigo 19º da Lei 58/2019, parece persistir a seguinte dúvida: **as mesas de restaurantes podem estar abrangidas por câmaras de um sistema de videovigilância?**

É certo que a videovigilância é lícita se for necessária para satisfazer os interesses legítimos prosseguidos pelo responsável pelo tratamento, ou seja, no caso em apreço, interesses legítimos do proprietário de um restaurante em implementar medidas de proteção de pessoas e bens.

Apesar disso, nas «Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo», o Comité Europeu para a Proteção de Dados (CEPD) afirma que as pessoas "também podem **ter a expectativa de não ser controlados no interior de espaços públicos, especialmente se esses espaços forem normalmente utilizados para atividades de (…) lazer, bem como em lugares onde os indivíduos permanecem e/ou comunicam, como (…) mesas de restaurantes**. Neste caso, os interesses ou direitos e liberdades do titular dos dados sobrepõem-se frequentemente aos interesses legítimos do responsável pelo tratamento" (negrito nosso).

No mesmo contexto, a Comissão Nacional de Proteção de Dados (CNPD) clarifica, no seu website, que as câmaras de videovigilância "**não podem incidir sobre o interior de áreas reservadas a clientes ou utentes, tais como: (…) salas de refeições, esplanadas (...)**" (negrito nosso).

Face ao exposto, parece existir um conflito entre a proteção de pessoas e bens e a proteção de dados pessoais! Mas, na realidade, ambas as "proteções" são compatíveis.

É sabido que existe obrigação legal de instalação de sistemas de videovigilância em discotecas, provavelmente, atendendo ao histórico de conflitos/crimes ocorridos nos acessos ou nos espaços ou salas destinados à dança, ou onde habitualmente se dance. Ou seja, os estabelecimentos de diversão noturna, entre outras medidas de segurança, são obrigados à instalação de um sistema de videovigilância. No entanto, essa obrigação legal não se aplica à generalidade dos restaurantes.

Na verdade, para a finalidade de proteção de pessoas e bens, basta que as imagens recolhidas se

refiram ao acesso ao interior de um restaurante, ou seja, consigam ser identificadas, as pessoas que entram e saem, com gravação exata do dia e hora. A prova que fica registada, poderá ser utilizada, em caso de necessidade, de acordo com o estabelecido em legislação para o efeito.

Em suma, em Portugal, atendendo à legislação em vigor e às diretrizes do Comité Europeu para a Proteção de Dados (as quais visam dar orientações sobre como aplicar o RGPD em relação ao tratamento de dados pessoais através de dispositivos de vídeo), conclui-se que, não existindo imposição legal para o efeito, as mesas da generalidade dos restaurantes **não podem** estar abrangidas por câmaras de um sistema de videovigilância.

Segurança e Privacidade 5.0

Visão geral *Direitos, Liberdades e Garantias | Segurança de pessoas e bens | Privacidade.*

Tendo sempre em mente o cumprimento do RGPD e legislação complementar, o projeto "Segurança e Privacidade 5.0" pretende contribuir para um maior esclarecimento da generalidade das entidades públicas e privadas, em matéria de proteção de dados, em especial, quanto à instalação/utilização de sistemas de videovigilância.

Paralelamente, o projeto "Segurança e Privacidade 5.0", com consultores experientes, disponibiliza soluções de auditoria e consultoria, tanto na fase de projeto como após a instalação/renovação de sistemas de videovigilância.

Em suma, o objetivo principal é alcançar o equilíbrio ponderado entre a proteção de dados e a segurança. Para mais informações, consulte-nos.

***Fundadores / Consultores**:*

Jorge Martinez Batalha

Fundador da SEGURANÇA E PRIVACIDADE 5.0; Consultor-Formador;

Encarregado da Proteção de Dados (DPO); Presidente do Conselho Fiscal da APDPO Portugal

https://www.linkedin.com/in/jmbatalhaconsultor/

Mário Peixinho

Fundador da SEGURANÇA E PRIVACIDADE 5.0; Data Privacy Advisor

https://www.linkedin.com/in/mariopeixinho/

A importância de ter um Data Protection Officer certificado

Ana Duarte

Knowledge | Product Manager

SGS

Atualmente, a proteção de dados e a segurança da informação, ao nível da confidencialidade, integridade, disponibilidade e resiliência dos dados pessoais, tem vindo a ser alvo de um contínuo processo de valorização e reconhecimento por força da entrada em vigor do Regulamento Geral sobre a Proteção de Dados e demais legislação aplicável, ganhando relevo nas organizações independentemente da sua dimensão, quer no âmbito do setor público, mas sobretudo, no setor privado.

Embora seja inegável que os dados pessoais são fonte de riqueza e lucro das organizações, temos vivido tempos sombrios no que diz respeito aos constantes e persistentes ataques informáticos sobre os órgãos da Administração Pública e demais empresas. Cada vez mais se justifica que este tema seja tratado com rigor e preocupação por parte de todas as entidades obrigadas à designação de um Encarregado da Proteção de Dados, ou o chamado Data Protection Officer (DPO).

O Encarregado de Proteção de Dados é, pela definição do RGPD, uma entidade livre e autónoma, e deve defender este estatuto, manifestando-se sempre que considere que não tem os meios para o exercício da sua função. Sem prejuízo do RGPD já prever uma linha orientadora sobre as qualificações a observar neste

profissional e a salvaguarda de quaisquer e eventuais conflitos de interesses por força do exercício orgânico e material das suas funções, posição e importância no seio da conformidade do tratamento dos dados e segurança de informação.

O dia a dia das organizações deve pautar-se pela tónica na preocupação com os dados pessoais objeto de tratamento efetuado por si sobre os dados dos seus clientes, mas também sobre os dados dos colaboradores.

A relevância da posição do Encarregado de Proteção de Dados tem por base as suas funções enquanto garante da conformidade, ao nível da informação, sensibilização e consciencialização do responsável pelo tratamento e/ou subcontratante, mas também dos trabalhadores que estejam em contacto com dados pessoais; controlo da conformidade com o RGPD e demais legislação aplicável; formação e sensibilização do pessoal implicado nas operações de tratamento de dados e auditorias correspondentes; aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlo da sua realização; e ser o ponto de contacto e entidade cooperante com a Comissão Nacional de Proteção de Dados.

Não convém esquecer que, na eventualidade de uma não conformidade ou ocorrência de qualquer violação de dados serão apuradas e imputadas responsabilidades ao responsável pelo tratamento e, em última instância, aos órgãos de gestão, nos casos de culpa ou dolo pelos incidentes e danos causados.

É importante que nos dias que correm, a velocidade da informação, a agilidade e necessidade premente do tratamento de dados, não se sobreponha aos mais elementares direitos fundamentais de cada cidadão enquanto titular dos dados.

Uma organização ou entidade em conformidade com o RGPD e demais legislação aplicável, em conjunto com as boas práticas associadas ao manuseamento dos dados, é sinónimo de boa reputação e credibilidade, sobretudo num mercado e espaço digital tão permeável volátil a ataques cibernéticos e violações de dados.

Precisamos de Encarregados da Proteção de Dados preparados para os constantes desafios, mas sobretudo, que as organizações tomem consciência da relevância da sua função.

É neste contexto que a SGS ICS se encontra em fase de desenvolvimento de uma nova certificação de pessoas: **Certificação para Encarregado de Proteção de Dados (DPO)**.

Esta especificação técnica define os requisitos do processo de certificação de pessoas por forma a assegurar que o processo de certificação é efetuado de

uma forma consistente e controlada, cumprindo os requisitos da norma ISO/IEC 17024:2012 e da sua posterior acreditação. O objetivo deste documento é estabelecer as regras gerais que regulam a certificação de pessoas da categoria Encarregado da Proteção de Dados.

A certificação de pessoas é um processo objetivo de avaliação de competências e um meio para garantir que as pessoas certificadas cumprem os requisitos deste esquema de certificação. O desenvolvimento desta certificação conta com uma comissão técnica multidisciplinar da qual a APDPO - Associação dos Profissionais de Proteção e Segurança de Dados é um dos membros.

A SGS ICS é o organismo de certificação do Grupo SGS. Os seus serviços de certificação permitem demonstrar que os produtos, processos, sistemas ou serviços estão em conformidade com as normas e regulamentos nacionais e internacionais. A SGS, empresa líder mundial em testes, inspeção e certificação, é reconhecida como uma referência global em sustentabilidade, qualidade e integridade. Em Portugal desde 1922, a SGS Portugal está presente em todo o território nacional, incluindo Açores e Madeira, através de uma rede de 12 escritórios e laboratórios.

SGS ACADEMY

A TRANSFORMAR PESSOAS E NEGÓCIOS

Encontre o seu caminho através da nossa formação

LINKEDIN

FACEBOOK

Para mais informações, contacte-nos:

808 200 747

PT.INFO@SGS.COM

LEARNING.SGS.COM/PT

SGS

Certificação em Sistemas de Gestão SGS

A SGS disponibiliza uma ampla gama de serviços de Auditoria e de Certificação de Sistemas de Gestão, para ajudar a sua empresa a melhorar o desempenho dos seus processos e sistemas, bem como para ajudar a comprovar a conformidade em toda a sua cadeia de valor.

Como fornecedor líder mundial em serviços de gestão de sistemas de certificação, oferecemos experiência, competência e recursos inigualáveis, garantindo a conformidade da sua organização com os requisitos regulatórios - onde quer que a sua empresa opere.

Podemos ajudá-lo a obter a Certificação em Sistemas de Gestão e a Certificação de Conformidade, alinhadas a uma ampla gama de normas de sistemas de gestão, entre as quais:

- **QUALIDADE: ISO 9001**
- **AMBIENTE: ISO 14001**
- **SEGURANÇA, HIGIENE E SAÚDE NO TRABALHO: ISO 45001**
- **SEGURANÇA ALIMENTAR: HACCP, ISO 22000**
- **SEGURANÇA DA INFORMAÇÃO: ISO 27001**

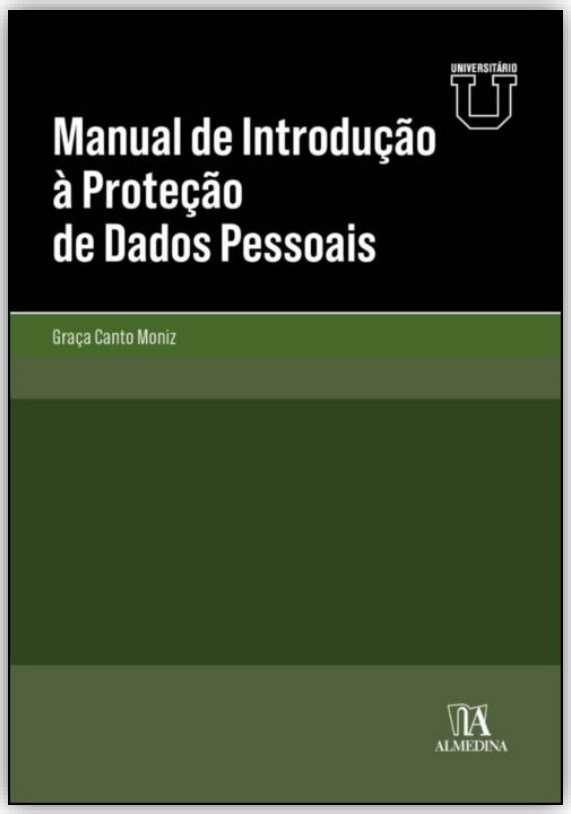
808 200 747
PT.INFO@SGS.COM
WWW.SGS.COM/PT-PT

SGS

Uma introdução ao regime geral de proteção de dados pessoais da União Europeia

Graça Canto Moniz

O Manual de Introdução à Proteção de Dados Pessoais publicado pela Almedina no início deste ano é um livro para quem procura uma introdução ao regime geral de proteção de dados pessoais da União Europeia, também conhecido com Regulamento Geral Sobre a Proteção de Dados Pessoais ou "RGPD". Este Manual é o resultado de apontamentos desenvolvidos que comecei a escrever para os vários cursos e programas de proteção de dados pessoais que coordenei e nos quais participo desde 2017. Entre 2019 e 2022 esses apontamentos foram desenvolvidos para servir de suporte à disciplina de Data Protection and Management Law, da qual fui regente na NOVA School of Law e, mais recentemente, são os elementos de apoio aos estudantes de Mestrado em Direito Público da disciplina Direito da Proteção de



Dados Pessoais, também da minha responsabilidade, na Faculdade de Direito da Universidade Lusófona.

O manual está dividido em 5 capítulos. O primeiro capítulo é introdutório: analiso a evolução, os objetivos, a natureza e o âmbito de aplicação do regime referido. Já no segundo capítulo debruço-me sobre os princípios aplicáveis ao tratamento de dados pessoais procurando, ao longo do estudo, citar decisões de autoridades de controlo e de tribunais que nos ajudem a compreendê-los. Noto que alguns princípios estão mais consolidados na prática jurídica – transparência, licitude e limitação da conservação – e outros há que suscitam (e continuarão a suscitar) dúvidas quanto aos seus limites e aplicação prática, em especial a lealdade, a integridade e confidencialidade e, sobretudo, a responsabilidade.

No capítulo que se segue apresento os vários atores relevantes neste regime e dou destaque ao entendimento do Tribunal de Justiça da União Europeia sobre a figura da responsabilidade conjunta, bem como às críticas de alguma doutrina estrangeira a esta posição. No fundo, a posição daquele Tribunal poderá suportar interpretações (demasiado) amplas sobre a responsabilidade pelo tratamento levando a um certo esvaziamento da figura da subcontratação. Ainda no mesmo capítulo, dou a minha opinião sobre a qualificação de alguns atores, em particular o caso dos médicos e das empresas de medicina no trabalho frequentemente consideradas como subcontratantes.

O quarto capítulo é dedicado aos direitos do titular dos dados e o último capítulo, o quinto, às obrigações previstas no regime estudado. Nos dois casos a abordagem é igual: analiso as disposições legais e recorro a decisões de autoridades de controlo e de tribunais para aprofundar aspetos concretos e perceber, na prática, como estão a ser aplicadas. No último capítulo, sigo a mesma abordagem sendo que, como concordarão a maior parte dos leitores deste texto, em relação a alguns temas é ainda difícil encontrar respostas precisas. Os exemplos são vários. Destaco, no que diz respeito à obrigação de gestão adequada dos riscos, a dificuldade em medir, de forma eficaz e objetiva, o risco na sua componente probabilística, referida nos considerandos 75 e 76 do RGPD e em normas que estipulam obrigações como o artigo 24.º, n.º 1, e 25.º, n.º 5. Esta dificuldade tem-se manifestado em situações em que o legislador impõe aos operadores a capacidade de distinguir entre um mero risco e um risco qualificado ou "elevado", por exemplo na determinação da comunicação de uma violação de dados pessoais ao titular.

Outro tema cuja evolução traço no capítulo 5 é o das transferências de dados pessoais. Há muitos anos que as instituições europeias reconhecem a insatisfação dos operadores com a complexidade do

regime das transferências que, desde a Diretiva 95/46/CE, pouco (quase nada) mudou. A saga Schrems não só veio demonstrar algumas insuficiências na capacidade desse regime para proteger, de forma eficaz, o titular dos dados como veio ainda acrescentar uma nova camada de incerteza e novos desafios aos operadores. Neste domínio há vários temas ainda em discussão, começando pela validade substancial da proposta de Decisão de Adequação dos Estados Unidos da América até ao papel do risco no regime das transferências de dados pessoais.

Em síntese, este não é um livro onde o leitor vai encontrar todas as respostas para os múltiplos problemas que estão hoje em cima das mesas de encarregados de proteção de dados, de advogados e de outro tipo de operadores nesta área. Ainda assim, há alguns temas que, pela sua importância e atualidade, são mais detalhados em resultado da minha experiência académica, mas também de reflexões com outros intervenientes em diferentes fóruns.

A responsabilidade civil do DPO

Rodrigo Adão da Fonseca

Co-CEO FUTURA

Introdução: A figura do "Data Protection Officer" ("DPO") ganhou relevância com o início da aplicação do Regulamento Geral de Proteção de Dados ("RGPD") na União Europeia em 2018. O RGPD estabelece, como é sabido de todos os que leem esta revista, a necessidade de designar um DPO em determinadas organizações que lidam com dados pessoais.

Neste artigo abordaremos as responsabilidades e tarefas do DPO, revisitaremos o princípio da responsabilidade do responsável pelo tratamento, a independência do DPO e, por fim, os riscos associados à responsabilidade civil do DPO, bem como a importância de dispor de um seguro adequado.

Responsabilidades e tarefas do DPO: O DPO é um profissional encarregado de garantir o cumprimento das leis e regulamentações de proteção de dados na organização para a qual é indigitado.

As suas principais responsabilidades incluem (cf. artigo 39.º do RGPD):

a) Informar e aconselhar a organização e os seus funcionários sobre suas obrigações em relação à proteção de dados;

b) Monitorar o cumprimento das políticas internas de proteção de dados e das leis aplicáveis;

c) Atuar como ponto de contato entre a organização e as autoridades regulatórias;

d) Realizar auditorias de proteção de dados e recomendar ações corretivas;

e) Apoiar na realização de avaliações de impacto sobre a proteção de dados, quando tal lhe for solicitado;

f) Colaborar com os "stakeholders" internos, como os departamentos jurídico, segurança da informação, compras, formação recursos humanos, auditoria interna e gestão do risco, para colocar o tema da proteção de dados na agenda da organização.

O princípio da responsabilidade face à independência do DPO: A responsabilidade do DPO é distinta da responsabilidade do responsável pelo tratamento. Esta ideia central nem sempre tem sido bem apreendida pelas organizações ou assimilada pelos DPO que frequentemente se deixam enredar por situações que os colocam perante inúmeros conflitos de interesse, difíceis de compatibilizar.

O responsável pelo tratamento tem a responsabilidade principal de garantir que os dados são tratados de acordo com o RGPD e outras leis aplicáveis, sendo quem determina os fins e meios do tratamento de dados pessoais (cf. artigos 24.º e 32.º do RGPD).

Já o DPO atua como um conselheiro e supervisor, mas não assume a responsabilidade pelos atos e omissões da organização no tratamento de dados. É importante ressaltar que, embora o DPO seja um agente de controle interno, ele não substitui a responsabilidade do responsável pelo tratamento em cumprir com o RGPD e outras leis aplicáveis.

A independência do DPO face ao responsável pelo tratamento é, aliás, fundamental para garantir a imparcialidade e a eficácia na supervisão do cumprimento das leis de proteção de dados. O RGPD estabelece, sem margem para dúvidas, que o DPO não deve receber instruções relacionadas ao exercício de suas funções, não podendo ser demitido ou penalizado por desempenhar suas tarefas (cf. n.º 3 do artigo 38.º do RGPD).

Mas não apenas: o DPO, ele próprio, deve mitigar conflitos de interesse, o que significa que deve furtar-se ao desempenho de funções que possam interferir com as suas responsabilidades, como as que são próprias do responsável pelo tratamento, evitando ao máximo estar envolvido em operações de tratamento de dados pessoais. Neste contexto, a organização deve criar as condições para evitar que o DPO seja colocado em situações de conflito de interesses. Mas também, o próprio DPO deve recusar as tarefas que ponham em causa a sua independência ou o coloquem perante um conflito de interesses, sempre que tal lhe seja inadvertidamente solicitado pela organização onde exerce funções.

Riscos em matéria de responsabilidade civil e a importância do seguro: Embora o DPO não seja diretamente responsável pelos atos e omissões da organização no tratamento de dados, tal não significa que da sua função não resultem responsabilidades profissionais,

nomeadamente em matéria de responsabilidade civil. O DPO pode sempre ser acionado por negligência, má conduta ou falha no cumprimento das suas obrigações profissionais. Além disso, o DPO pode ser responsabilizado por danos causados a terceiros, como titulares de dados, se for estabelecido que suas ações ou omissões contribuíram para uma violação de dados ou para o não cumprimento das leis de proteção de dados.

Neste contexto, é crucial que o DPO possua uma cobertura de seguro adequada para se proteger contra riscos de responsabilidade civil. Um seguro de responsabilidade civil profissional pode ajudar a mitigar os riscos financeiros associados a reclamações e ações judiciais decorrentes de erros, omissões ou negligências no exercício de funções. Essa cobertura é especialmente importante, dado o potencial de sanções e multas significativas impostas pelas autoridades reguladoras, bem como a crescente conscientização dos titulares de dados sobre seus direitos e a probabilidade de buscarem compensação por danos. Sendo a nossa profissão, de elevado risco pessoal, sempre que me é perguntado, recomendo aos colegas DPO a contratação de um seguro de responsabilidade civil profissional adequado, por considerar que tal é uma medida crucial para mitigar os riscos financeiros e legais que enfrentamos no exercício da nossa atividade.

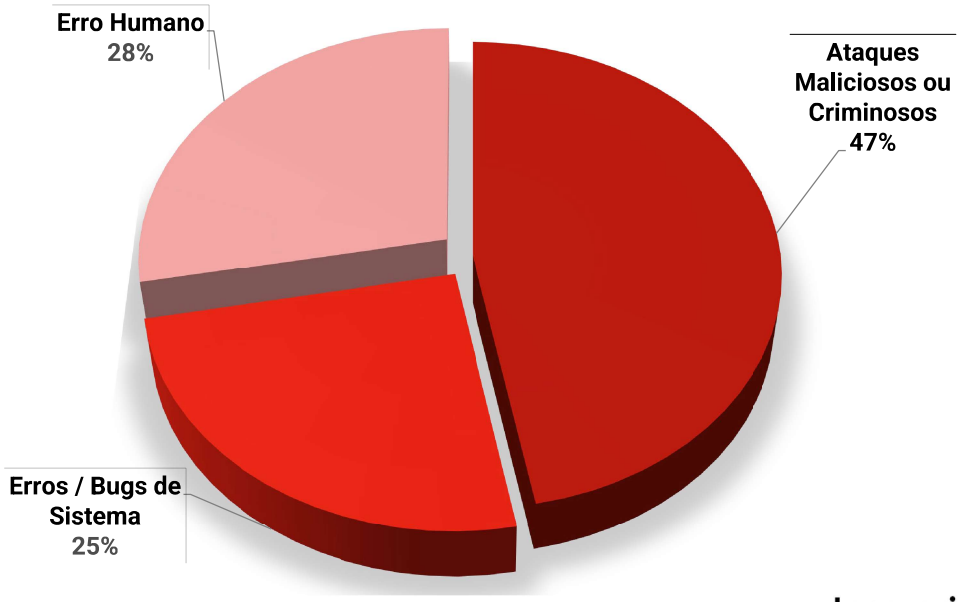
Riscos Globais:

- Todas as empresas utilizam **Tecnologia** e **Internet**
- A **globalização** da atividade económica expõe as empresas a um número cada vez maior de geografias e realidades locais
- As **ameaças à segurança informática e tecnológica** podem vir de qualquer parte do mundo
- O crime informático cresce em todo o mundo a uma **velocidade sem paralelo**, bem como a complexidade e as alterações na atividade económica.

Risco de Continuidade:

- Uma pequena **Empresa pode fechar** devido a um ataque
- Uma grande Empresa pode ter um impacto direto na sua **reputação**
- Os DPO's acabam por ter, direta e indiretamente, muita **influência na defesa da Empresa**

PRINCIPAIS CAUSAS DOS ATAQUES



Fonte: Hiscox Europe 2022

SEGURO DE RESPONSABILIDADE CIVIL PARA DPO'S

O seguro de responsabilidade Civil para DPO's protege-os perante **erros ou omissões** durante a sua atividade profissional baseados em:

- Negligência
- Quebra de confidencialidade
- Direitos de propriedade intelectual
- Práticas desleais
- Difamação
- Custos de defesa
- Responsabilidade contratual e extracontratual

Os associados da APDPO têm acesso a **condições exclusivas** para Profissionais Independentes e Empresas.

Não dispensa a consulta da informação pré-contratual e contratual legalmente exigida.

CONTACTOS GERAIS

AON Portugal

Av. Da Liberdade 249, 2º
1250-143 Lisboa
PORTUGAL

Website: Aon Portugal
Email geral: suporte.seguros@aon.pt
Telefone: 808 50 50 70 (dias úteis até às 17h)