INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

A proteção de dados pessoais – auditoria e controlo interno no âmbito das competências da Inspeção Nacional da Polícia de Segurança Pública.

Auditor
Luís Manuel Carvalho da Silva

Trabalho Individual Final
VI – CDEP

Orientação científica
Professor Doutor Pedro José Lopes Clemente

Setembro, 2024

Agradecimentos

Gostaria de expressar o meu mais profundo agradecimento a todas as pessoas e instituições que tornaram possível a concretização deste projeto.

Ao Professor Doutor Pedro José Lopes Clemente, pela prontidão e disponibilidade em aceitar ser o meu orientador. A sua paciência, serenidade e compreensão foram fundamentais para que eu me mantivesse alinhado com os eixos centrais do trabalho. Agradeço profundamente pelos seus vastos conhecimentos científicos e académicos, que foram essenciais ao longo de todo o processo, enriquecendo-me tanto a nível pessoal quanto profissional.

À Dr.ª Alexandra Maria De Carvalho Teixeira Gomes, da Inspeção Nacional da PSP, pela incansável boa disposição, disponibilidade e apoio. A troca de conhecimentos com ela foi uma experiência única e enriquecedora.

À Polícia de Segurança Pública pela oportunidade de desenvolvimento pessoal que o CDEP possibilitou na minha carreira policial.

Ao Instituto Superior de Ciência Policias e Segurança Interna, a minha casa académica, pelo acolhimento, apoio e colaboração, permitindo que este trabalho se concretizasse, em especial a todos os seus colaboradores, cujo contributo foi inestimável.

Aos professores do Instituto e convidados, pelo inestimável apoio e orientação ao longo do VI CDEP. O vosso compromisso e dedicação foram fundamentais para a concretização deste objetivo.

Aos colegas de mestrado, em especial à Mónica, pelo companheirismo, apoio e amizade demonstrados, que tornaram este percurso mais leve e agradável.

A todos os amigos, colegas e conhecidos, que de alguma forma contribuíram para este projeto, mesmo sem o saberem, servindo como fonte de inspiração e motivação nos momentos mais desafiantes.

Por fim, e com especial destaque, à Filomena, a mulher da minha vida e aos nossos filhos: André, Rita e Maria. A vossa paciência perante as minhas ausências, o vosso constante incentivo, apoio psicológico e emocional, foram a base que me sustentou durante este percurso. Agradeço-vos pela vossa força, pelo carinho incondicional, pela fé que sempre depositaram em mim, e por me darem a coragem necessária para seguir em frente. Este projeto é tanto meu quanto vosso.

Resumo

A proteção de dados pessoais é crucial para entidades que gerem informações sensíveis, como a Polícia de Segurança Pública (PSP). Este estudo avalia as práticas de auditoria e controlo interno da PSP, com foco no cumprimento do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (EU). Através de uma metodologia qualitativa incidindo na análise documental, investiga-se a implementação das políticas de proteção de dados e os desafios enfrentados.

As questões principais incluem a adequação das práticas da PSP às exigências do RGPD e o impacto dessas práticas na segurança e integridade dos dados pessoais geridos. O estudo também explora a implementação de medidas de conformidade, identificando obstáculos e oportunidades de melhoria.

Pesquisas preliminares indicam que, embora a PSP tenha progredido na adaptação ao RGPD, há áreas críticas a serem melhoradas, como a formação do efetivo, a implementação e o uso de tecnologias de proteção avançada e o reforço dos mecanismos de monitorização e avaliação de conformidade com o Regulamento.

Este estudo destaca a importância de uma abordagem proactiva na proteção de dados, evidenciando a importância da Inspeção Nacional (IN) bem como do Encarregado de Proteção de Dados (EPD), apresentado recomendações para fortalecer as práticas de auditoria e controlo interno na PSP.

Palavras-chave: Polícia, Proteção de dados, Auditoria Interna, Inspeção

Abstrat

The protection of personal data is crucial for entities that manage sensitive information, such as the Public Security Police (PSP). This study evaluates the PSP's auditing and internal control practices, with a focus on compliance with the European Union's General Data Protection Regulation (RGPD). Through a qualitative methodology focusing on documentary analysis, the implementation of data protection policies and its challenges are investigated.

The key issues examined include the adequacy of the PSP's practices to the requirements of the RGPD and the impact of these practices on the security and integrity of the personal data managed. The study also explores the implementation of compliance measures, identifying obstacles and opportunities for improvement.

Preliminary research indicates that, although the PSP has made progress in adapting to the RGPD, there are critical areas for improvement, such as the training of staff, the implementation and use of advanced protection technologies and the strengthening of mechanisms for monitoring and evaluating compliance with the Regulation.

This study highlights the importance of a proactive approach to data protection, highlighting the importance of the National Inspectorate (IN) as well as the Data Protection Officer (EPD), and provides recommendations to strengthen audit and internal control practices in the PSP.

Keywords: Police, Data Protection, Internal Audit, Inspection

Índice

Introdução ... 7

1. Conceptualização ... 11

1.1. Proteção de Dados Pessoais ... 11

1.1.1. Evolução europeia da Proteção de Dados Pessoais ... 11

1.1.2. A Proteção de Dados Pessoais em Portugal ... 15

1.1.3. A Proteção de Dados Pessoais na PSP ... 16

1.2. Auditoria Interna e Controlo Interno ... 17

1.2.1. Auditoria Interna ... 18

1.2.2. Controlo Interno ... 18

2. A auditoria e controlo interno na PSP ... 19

2.1. Inspeção Nacional ... 19

2.2. Departamento de Gestão Financeira ... 20

3. Encarregado de Proteção de Dados ... 21

3.1. O Estatuto do EPD ... 21

3.2. Obrigatoriedade e Condições de designação ... 22

3.3. Responsabilidades do EPD ... 23

4. Síntese conclusiva ... 23

4.1. Procedimentos de conformidade ... 23

4.2. Prevenção de Violações do RGPD e Conformidade Legal ... 25

4.3. Compatibilidade das Competências do EPD e da IN ... 26

4.3.1. Áreas de atuação compatíveis ... 27

4.3.2. Áreas de atuação diferenciada ... 27

4.4. Riscos de Incompatibilidade ... 28

4.5. Medidas de mitigação e eliminação de riscos de incompatibilidade ... 28

Conclusão ... 31

Bibliografia ... 34

Lista de Abreviaturas

AEPD – Autoridade Europeia para a Proteção de Dados

AI – Auditoria Interna

AIPD – Avaliação de Impacto sobre Proteção de Dados

CE – Comissão Europeia

CEPD – Comité Europeu para a Proteção de Dados

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

DGF – Departamento de Gestão Financeira

DIC – Departamento de Investigação Criminal

DN – Diretor Nacional

DSIC – Departamento de Sistemas de Comunicação e Informação

EEE – Espaço Económico Europeu

EPD – Encarregado de Proteção de Dados

GAI – Gabinete de Apoio à Inspeção

GAJ – Gabinete de Assuntos Jurídicos

IN - Inspeção Nacional da PSP

IPAI – Instituto Português de Auditoria Interna

IIPA – The Institute of Auditors

NAI – Núcleo de Auditoria Interna

NATI – Núcleo de Assessoria Técnica à Inspeção

PIIC – Plataforma para o Intercâmbio de Informação Criminal

PSP – Polícia de Segurança Pública

RGPD – Regulamento Geral de Proteção de Dados

SCI – Sistema de Controlo Interno

SEI – Sistema Estratégico de Informação

UE – União Europeia

Introdução

A proteção de dados pessoais está na ordem do dia, quer pela consciência da necessidade de garantir os direitos, liberdades e garantias dos cidadãos, quer pela consciência coletiva e institucional de que, com a evolução tecnológica e pela afirmação da Inteligência Artificial, cada vez mais o indivíduo pode estar em risco devido à violação dos seus dados pessoais.

Para essa consciencialização contribui a pressão da UE, pelo desenvolvimento de uma estratégia de imposição de normas de controlo e garantia de defesa da proteção de dados dos cidadãos, no sentido de serem adotadas medidas objetivas de proteção de dados pessoais no espaço europeu e nas ações diretamente relacionadas com cidadãos europeus, em certas circunstâncias mesmo fora do espaço europeu.

A proteção de dados pessoais, particularmente em instituições públicas responsáveis pela segurança nacional, entre as quais se destaca a PSP, é um tema de importância crescente e urgente, pois terão, neste novo quadro legal, de se adaptar, promovendo as medidas técnicas e organizacionais que permitam o cumprimento das suas múltiplas missões garantindo a proteção dos dados pessoais dos cidadãos.

A análise do regime de legal de proteção de dados pessoais aplicável à atividade policial é complexa e envolve uma panóplia de normativos legais, sendo que o ponto de viragem mais importante da última década deu-se em 2016, com a aprovação do RGPD[1] em 27 de abril de 2016, com início de vigência em 25 de maio de 2018, seguindo-se a publicação da Lei n.º 58/2019[2], de 08 de agosto, para sua execução.

Moreira (2018) na sua tese de mestrado ao analisar o RGPD refere que

> "o objetivo principal, não será o de dotar as organizações de ferramentas para se protegerem, mas sim, o de proteger todo e qualquer titular de dados pessoais" (p.5).

O RGPD vem alterar o paradigma da proteção de dados pois centra a defesa da proteção de dados nos seus titulares e não nas organizações enquanto utilizadores de dados de pessoas com as quais tenham tido ou venham a ter interação de qualquer natureza (Moreira, 2018).

A falta de doutrina interna, na PSP, sobre proteção de dados em geral, e sobre o RGPD em especial, é crítica, atendendo à evolução da sociedade na defesa dos direitos dos

---

[1] RGPD - (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicado no Jornal Oficial da União Europeia, em 4 de maio de 2016.

[2] Lei n.º 58/2019, de 8 de agosto, lei de execução do RGPD em Portugal, publicada no Diário da República (DR) n.º 151/2019, Série I de 2019-08-08, páginas 3 – 40.

cidadãos, no quadro da defesa dos direitos humanos, exigindo-se cada vez mais transparência à administração pública, que a PSP integra, pelo que a necessidade permanente da avaliação de riscos será fundamental para o cumprimento da legislação e para garantir que a organização não é colocada em situação de incumprimento, não permitindo que a violação de dados pessoais possa colocar os cidadãos em risco e a reputação da PSP em causa.

Na PSP os estudos sobre o RGPD e as suas implicações na qualidade do serviço policial prestado aos cidadãos não foram, até ao momento, alvo de grande atenção, sendo relevante o estudo efetuado por Arvelos (2023), onde analisou algumas "atividades diárias da PSP e o eventual (in)cumprimento do RGPD, com todos os constrangimentos que se deparam, numa estrutura fortemente hierarquizada em que a mudança é sempre lenta".

É destes constrangimentos e de uma aparente incapacidade da PSP em cumprir o RGPD, que surge a oportunidade de, através do quadro legal existente, onde a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, transposta para o ordenamento jurídico português pela Lei n.º 59/2019 [3], de 08 de agosto, que veio estabelecer as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, a IN e o EPD assumirem um papel relevante.

Neste estudo tentaremos verificar de que forma o sistema de auditoria e controlo internos da IN que, pela sua natureza e funções, são cruciais para a garantia da legalidade, eficiência e transparência de todas as atividades da PSP, será ou não preventiva e de correção de processos e procedimentos, garantindo a prestação de um serviço de qualidade e excelência, respeitando os direitos liberdades e garantias (Moreira, 2018).

Esta "auditoria permanente" (Saldanha, 2019) poderá ser fundamental para que, de possíveis falhas no tratamento e gestão de dados pessoais, promovidos pela PSP, não venha a resultar responsabilidade civil, penal ou contraordenacional por parte dos responsáveis pela gestão e tratamento dos dados pessoais, por incumprimento dos parâmetros legais e constitucionais.

No contexto atual, onde a informação se transformou num dos bens mais valiosos e sensíveis, a questão da segurança e privacidade desses dados torna-se um campo fértil para estudos académicos e aplicações práticas, pelo que este estudo visa entender não apenas as

[3] Lei n.º 59/2019, de 8 de agosto, Transposição da Diretiva da União Europeia sobre o tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, publicada no DR n.º 151/2019, Série I de 2019-08-08, páginas 41 – 68.

políticas e práticas atuais relacionadas com a proteção de dados pessoais na PSP, mas também avaliar a eficácia das estratégias de controlo interno e auditoria que suportam o cumprimento do RGPD e demais regulamentações aplicáveis.

O objeto deste estudo foca-se na dicotomia entre a atuação policial balizada pela ação de controlo da IN e a aplicabilidade das normas legais, em especial decorrentes do RGPD e da Lei n.º 59/2019, que introduz uma nova realidade jurídica, onde o EPD tem um papel estratégico na ação da PSP, no que concerne à fiscalização e auditoria das normas de tratamento de dados pessoais.

Constituindo-se o RGPD como um marco legal incontornável destinado a proteger os dados pessoais e a privacidade dos cidadãos na UE e no Espaço Económico Europeu, este estudo visa explorar o alinhamento das práticas da PSP com as exigências do RGPD, identificando os principais desafios e oportunidades para melhorar a conformidade regulamentar e a proteção de dados pessoais na sua interação com os cidadãos.

Neste quadro coloca-se a questão central (QC) de saber de que forma as práticas de auditoria e controlo interno da IN da PSP estarão alinhadas com as exigências do RGPD.

A investigação visa responder à questão central verificando de que forma as ações de auditoria e controlo interno estão asseguradas e implementadas na PSP para a proteção de dados pessoais, nas atividades da instituição, com especial atenção ao cumprimento do RGPD, em três vertentes, respondendo às seguintes questões derivadas (QD):

- QD1 – de que forma a proteção de dados pessoais é assegurada nas diversas atividades da PSP, que mecanismos e procedimentos garantem a conformidade com o RGPD e legislação conexa;
- QD2 – de que forma as ações de auditoria e controlo interno estão estruturadas e implementadas na PSP para prevenir violações do RGPD, legislação conexa, e assegurar a sua observância;
- QD3 – e de que forma as competências da IN são ou não compatíveis com as competências do EPD.

Teremos assim como objetivos específicos:

- avaliar a eficácia dos procedimentos de controlo interno adotados pela PSP;
- identificar e avaliar possíveis riscos de violação do RGPD e legislação conexa;
- identificar oportunidades de melhoria nos processos e procedimentos da PSP;

- recomendar medidas corretivas e preventivas para mitigar riscos e melhorar o desempenho da PSP em matéria de proteção de dados pessoais.

Para atingir os objetivos a que nos propomos a metodologia de investigação que adotámos será uma metodologia mista, combinando elementos de estudo de caso e de análise documental. Esta abordagem permitirá um exame detalhado tanto dos processos práticos quanto das políticas teóricas e regulamentares em vigor na PSP.

Começaremos por uma revisão da literatura com o objetivo de estabelecer uma base teórica sólida sobre a proteção de dados, auditoria e controlo interno, e compreender as especificidades legais e operacionais aplicáveis à PSP. Para o efeito será efetuada pesquisa e análise de literatura académica, legislação pertinente, como o RGPD, a Lei n.º 58/2019 e a Lei n.º 59/2019, ambas de 8 de agosto e estudos anteriores relevantes.

Dos elementos da metodologia de estudo de caso destacaremos o objetivo de analisar como a PSP implementa as políticas de proteção de dados e as práticas de auditoria e controlo interno.

No que concerne à análise documental o objetivo será examinar documentos internos da PSP para avaliar a conformidade com o RGPD e a eficácia do controlo interno.

Este estudo é crucial tanto para a PSP como para a sociedade em geral, numa era dominada pela inteligência artificial e pela digitalização massiva. Ao focar-se na conformidade com o RGPD, a investigação promove uma PSP mais transparente, confiável e responsável na proteção dos dados pessoais dos cidadãos.

1. Conceptualização

1.1. Proteção de Dados Pessoais

Com a evolução das tecnologias de informação, a sociedade moderna tem sido forçada a uma rápida e contínua adaptação às soluções tecnológicas inovadoras que sustentam a vida em comunidade. Essa realidade obriga a que os indivíduos, enquanto cidadãos com deveres e direitos, se adaptem com uma rapidez que não era exigida até então. De acordo com Andrade (2020), o direito à proteção de dados surge como uma das expressões mais sensíveis da relação entre o cidadão e as instituições públicas, nas sociedades democráticas, exigindo garantias adicionais na era digital.

Nesse contexto, a proteção de dados pessoais tornou-se um imperativo, tanto devido à crescente conscientização da necessidade de garantir os direitos, liberdades e garantias dos cidadãos, quanto pela preocupação coletiva e institucional com os riscos decorrentes do avanço tecnológico e da crescente presença da Inteligência Artificial (Arvelos, 2023), que expõem o indivíduo a potenciais violações de dados pessoais. A UE tem-se posicionado como um dos principais agentes de promoção de um quadro legal robusto e coerente para a proteção de dados pessoais no espaço europeu.

1.1.1. Evolução europeia da Proteção de Dados Pessoais

Embora a proteção de dados pessoais tenha hoje um enquadramento jurídico bem definido, esta preocupação tem sido uma constante ao longo do tempo, evoluindo à medida que a sociedade se desenvolve, como refere Vaz (2018),

> O direito à "privacy" foi autonomizado pela primeira vez em 1890, quando Samuel Warren e Louis Brandeis publicaram, na Harvard Law Review, um artigo sob o título "The Right to Privacy" (CASTRO, 2005, p. 17). Hoje, é tomado pelo nosso ordenamento jurídico como um verdadeiro direito fundamental, positivado nos artigos n.º 26º da CRP e 80º do CC. Por outro lado, nos EUA, ainda se compreende a privacidade segundo a definição de Warren e Brandeis, isto é, como "the right to be let alone". Igualmente, o artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º 1 do TFUE preveem o direito dos cidadãos à proteção dos seus dados pessoais.

Desde então, o conceito evoluiu até ser reconhecido como um direito fundamental na Declaração Universal dos Direitos Humanos de 1948 e na Convenção Europeia dos Direitos Humanos de 1950, que estabelecem a proteção contra interferências arbitrárias na vida privada, familiar e pessoal (Saldanha, 2019).

Com o tempo, o rápido desenvolvimento das tecnologias de informação e a globalização da economia digital tornaram necessário um quadro jurídico mais robusto e atualizado, culminando na adoção do RGPD pelo Conselho, em 27 de abril de 2016, com plena vigência a partir de 25 de maio de 2018 (Moreira, 2018).

A evolução da Proteção de Dados na UE tem sido constante, tendo a adoção da Diretiva 95/46/CE pela UE sido um marco inicial na proteção de dados pessoais, estabelecendo princípios fundamentais para o tratamento de dados no espaço europeu e garantindo a harmonização das legislações entre os Estados-membros (Vaz, 2018).

De acordo com Saldanha (2019),

> Em 1959, com a criação do Tribunal Europeu dos Direitos do Homem, a proteção dos direitos individuais ficou definitivamente consagrada quando o próprio tribunal esclareceu que o artigo 8.º da CEDH obrigava não só os Estados a absterem-se de praticar atos suscetíveis de violarem os direitos aí consagrados, como impôs uma atitude positiva por forma a garantirem o respeito efetivo pela vida familiar e privada.

Esse princípio é respaldado tanto pelo Pacto Internacional dos Direitos Civis e Políticos quanto pela Convenção Europeia dos Direitos Humanos. Mais tarde, a Convenção 108 do Conselho da Europa, essencial para a proteção de dados pessoais em sistemas automatizados, serviu de base para a Diretiva 95/46/CE, que integrou princípios como a finalidade, a adequação e a pertinência no tratamento desses dados.

É essencial destacar o papel fundamental da Carta dos Direitos Fundamentais da União Europeia, que, nos seus artigos 7.º e 8.º, reconhece o respeito pela vida privada e a proteção de dados pessoais como direitos fundamentais, intimamente relacionados, mas distintos. A Carta também prevê o cumprimento das regras nela estabelecidas, bem como a sua supervisão por uma autoridade independente (Carta dos Direitos Fundamentais da UE, 2012).[4]

O direito à proteção de dados pessoais tem assim origem no direito à privacidade, conforme definido na Diretiva 95/46/CE (1995) e reforçado pelo RGPD. Não sendo, contudo, um direito absoluto, deve ser harmonizado com outros direitos fundamentais e aplicado de maneira proporcional.

A Diretiva 95/46/CE pode ser vista como o ponto de partida para a proteção de dados pessoais na UE, pois definiu os princípios essenciais que devem ser seguidos no

---

[4] Em Portugal a autoridade independente que garante o cumprimento do RGPD é a Comissão Nacional de Proteção de Dados (CNPD).

tratamento de dados pessoais. Ela serviu como a base legal que viabilizou o fluxo de dados no mercado único europeu, além de ter harmonizado as legislações de proteção de dados entre os Estados membros da UE.

Os principais objetivos da Diretiva 95/46/CE incluíam:

- Estabelecer um conjunto de regras para garantir que o processamento de dados pessoais seja realizado de forma justa e legal;
- Proteger os direitos e liberdades fundamentais das pessoas físicas, especialmente o direito à privacidade;
- Regular a transferência de dados pessoais para países fora da UE, garantindo um nível adequado de proteção;
- Estabelecer obrigações para os controladores de dados (entidades ou indivíduos que determinam as finalidades e meios de processamento de dados) e os processadores de dados (entidades que processam dados em nome do controlador);
- Criar mecanismos para que os indivíduos possam exercer seus direitos de acesso, retificação e eliminação de seus dados pessoais.

O RGPD substituiu a Diretiva 95/46/CE com uma legislação mais moderna e abrangente fortalecendo significativamente a proteção dos dados pessoais na UE, introduzindo novos direitos para os indivíduos, como o direito ao esquecimento e a portabilidade dos dados, e impondo obrigações rigorosas às organizações que realizam o processamento de dados pessoais (Vaz, 2018).

Para além de garantir um nível elevado de proteção de dados em toda a UE, o RGPD visa promover a confiança no uso de dados pessoais no contexto das atividades humanas, hoje em especial nas atividades digitais, um desafio crescente na era da Inteligência Artificial.

Os principais objetivos do RGPD incluem:

- Proteção dos Dados Pessoais: garantir um nível elevado de proteção dos dados pessoais dos cidadãos da UE.
- Direitos Individuais: reforçar os direitos dos titulares dos dados, como o direito de acesso, retificação, apagamento e portabilidade dos seus dados pessoais.

- Responsabilidade e Prestação de Contas: promover a responsabilidade e a transparência no tratamento de dados pessoais por parte das organizações, com a obrigação de implementar medidas adequadas de proteção.
- Consentimento Informado: reforçar as condições para obtenção do consentimento para o tratamento de dados, exigindo que seja livre, específico, informado e inequívoco.
- Notificação de Violações: estabelecer a obrigação de notificar as autoridades competentes e os titulares dos dados em caso de violações de segurança que possam comprometer a proteção dos dados pessoais.
- Sanções e Penalidades: estabelecer sanções e penalidades significativas para organizações que violem as disposições do RGPD, visando dissuadir práticas inadequadas de tratamento de dados.

Esses objetivos têm como finalidade assegurar um ambiente mais sólido e harmonizado de proteção de dados em toda a UE, reforçando a confiança dos cidadãos no tratamento de suas informações pessoais.

É importante destacar que o RGPD protege exclusivamente as pessoas físicas, independentemente da sua nacionalidade ou local de residência, no que diz respeito ao tratamento dos seus dados pessoais, não se aplicando ao tratamento de dados pessoais de pessoas jurídicas. Está também excluído o tratamento de dados realizado por indivíduos em atividades estritamente pessoais ou domésticas, sem vínculo com atividades profissionais ou comerciais. Ainda assim, o RGPD aplica-se aos responsáveis pelo tratamento e aos subcontratantes que fornecem os meios para o processamento de dados pessoais nessas atividades pessoais ou domésticas.

O RGPD também se aplica a todas as entidades que lidam com o tratamento de dados pessoais, sejam responsáveis pelo tratamento ou subcontratantes, em atividades tanto privadas quanto públicas. Para apoiar, acompanhar e fiscalizar a implementação e aplicação do RGPD, os países da UE instituíram órgãos nacionais encarregados da proteção de dados pessoais, conforme o artigo 8.º, n.º 3, da Carta dos Direitos Fundamentais da UE. Em Portugal, foi criada a CNPD para desempenhar esse papel.

O Comité Europeu para a Proteção de Dados (CEPD) é um órgão independente da UE que garante a aplicação uniforme das regras de proteção de dados em todo o território da UE. Criado pelo RGPD, o CEPD é composto por representantes das autoridades nacionais de proteção de dados dos países da UE/EEE e pela Autoridade Europeia para a

Proteção de Dados (AEPD). A Comissão Europeia (CE) participa nas atividades e reuniões do comité, porém sem direito a voto. O secretariado do CEPD é assegurado pela AEPD, atuando sob a direção exclusiva do presidente do comité.

As principais funções do CEPD incluem emitir orientações gerais sobre conceitos fundamentais do RGPD e da Diretiva (UE) 2016/680, aconselhar a CE em questões ligadas à proteção de dados pessoais e a novas legislações propostas na UE, além de adotar decisões vinculativas em disputas entre autoridades nacionais de supervisão.

Esta diretiva, também conhecida como Diretiva sobre a Proteção de Dados na Aplicação da Lei, estabelece regras específicas para o tratamento de dados pessoais por autoridades competentes com o objetivo de prevenir, investigar, detetar ou reprimir infrações penais, bem como para a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Assegura a proteção adequada dos dados pessoais de vítimas, testemunhas e suspeitos de crimes, facilitando a cooperação transfronteiriça no combate à criminalidade e ao terrorismo.

1.1.2. A Proteção de Dados Pessoais em Portugal

No ordenamento jurídico português, o direito à vida privada é um dos direitos fundamentais garantidos pela Constituição da República Portuguesa (CRP), consagrado no capítulo dos Direitos, Liberdades e Garantias, em particular nos artigos 26.º, n.º 1 e 35.º da CRP.

O artigo 26.º, n.º 1 da CRP assegura a proteção da intimidade da vida privada, garantindo a cada pessoa o direito de controlar a divulgação e o acesso a informações pessoais.

Por outro lado, o artigo 35.º da CRP garante aos cidadãos, na utilização da informática, o direito de acesso, de retificação e atualização dos seus dados pessoais, bem como o direito de conhecer a finalidade a que se destinam, conferindo proteção contra o uso indevido e abusivo de dados pessoais no contexto da tecnologia e da informação.

Essas disposições refletem o compromisso do sistema jurídico português em resguardar a dignidade e a autonomia dos indivíduos em relação à sua vida privada e ao uso das novas tecnologias (Moreira, 2018).

A CRP foi a primeira Constituição Europeia a consagrar a proteção de dados pessoais, uma vez que, já em 1976, o artigo 35.º da Constituição incorporava um direito especial de personalidade, com o objetivo de proteger os cidadãos contra os riscos decorrentes do uso da informática e de possíveis violações ao direito à privacidade.

Após esta análise histórica, podemos traçar um paralelismo entre a evolução da proteção de dados pessoais em Portugal e o desenvolvimento da mesma na UE.

Em Portugal, a proteção de dados pessoais passou a ser tratada em legislação específica com a promulgação da Lei n.º 10/91, de 29 de abril, que estabeleceu o marco legal fundamental para a proteção de dados pessoais no país, pois definiu os princípios essenciais para o tratamento de dados pessoais e estabeleceu as obrigações das entidades responsáveis pelo processamento desses dados.

Posteriormente, a Lei n.º 67/98, de 26 de outubro, transpôs a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, para o ordenamento jurídico português, que regulava a proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados. A lei representou um avanço importante, alinhando a legislação portuguesa com as normas europeias e estabelecendo um quadro mais abrangente para a proteção de dados pessoais em Portugal.

A proteção de dados pessoais também foi abordada pela Lei n.º 46/2012, de 29 de agosto, que regulou o tratamento de dados pessoais no contexto da prevenção, investigação, deteção ou repressão de infrações penais, bem como da execução de sanções penais.

No entanto, o marco mais significativo na proteção de dados pessoais em Portugal e na UE foi a entrada em vigor do RGPD, em 25 de maio de 2018, ao introduzir um conjunto abrangente de normas sobre o tratamento de dados pessoais nos Estados-membros da UE, incluindo Portugal, marcando um importante avanço na proteção dos direitos dos cidadãos.

A Lei n.º 58/2019, de 8 de agosto, garantiu a execução do Regulamento (UE) 2016/679, no ordenamento jurídico português, assegurando, na prática, a sua execução em Portugal.

Além disso, a Lei n.º 59/2019, de 8 de agosto, estabeleceu regras sobre o tratamento de dados pessoais para fins de prevenção, deteção, investigação ou repressão de infrações penais ou da execução de sanções penais, transpondo a Diretiva (UE) 2016/680, para a legislação portuguesa, garantindo a sua aplicação.

1.1.3. A Proteção de Dados Pessoais na PSP

Na PSP, os estudos sobre o RGPD e suas implicações na qualidade do serviço policial prestado aos cidadãos não têm recebido grande atenção até ao momento.

Nesse contexto, o estudo realizado por Arvelos (2023) destaca-se pela análise efetuada às “atividades diárias da PSP e o eventual (in)cumprimento do RGPD, com todos

os constrangimentos que se deparam, numa estrutura fortemente hierarquizada em que a mudança é sempre lenta".

É diante desses constrangimentos e da "aparente incapacidade" da PSP em cumprir o RGPD que surge a oportunidade de, com base no quadro legal existente, mormente na Lei n.º 59/2019, de 8 de agosto, que estabeleceu as regras para o tratamento de dados pessoais para fins de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, a PSP fortalecer de forma proativa as relações de confiança com os cidadãos aumentando o sentimento de segurança, contribuindo para uma sociedade mais inclusiva e segura.

O cumprimento da lei jamais poderá ser um obstáculo à garantia dos direitos, liberdades e garantias em geral, especialmente no que se refere à proteção de dados pessoais, conforme destacado por Monteiro (2021)

As leis da proteção de dados são um complemento à garantia de controlo dos dados dos titulares e à sua privacidade, e não uma limitação ao exercício das funções e atribuições das forças e serviços de segurança, como está, de resto, patente na Lei n.º 59/2019.

As autoridades e poderes públicos que tenham como atribuições e competências a prevenção, a deteção, a investigação e a repressão de ameaças à segurança pública, não estão limitados pela presente lei no que respeita à persecução da sua atividade.

A nomeação do EPD marcou um passo decisivo para o cumprimento do RGPD pela PSP. A designação do IN da PSP [5] para essa função foi especialmente significativa, demonstrando o compromisso da instituição em atribuir grande importância à sua política de privacidade no relacionamento com os cidadãos. Esse compromisso abrange tanto o público externo, principal destinatário das ações policiais, sejam elas preventivas ou reativas, quanto o público interno, que inclui os colaboradores da instituição, independentemente da sua relação jurídico-funcional com a PSP.

1.2. Auditoria Interna e Controlo Interno

Para obter melhores resultados com os recursos disponíveis, é cada vez mais importante considerar parâmetros como a eficácia no cumprimento dos objetivos e a eficiência na utilização de recursos escassos. Isso impõe aos gestores das organizações públicas um conhecimento mais profundo sobre o desempenho das suas atividades.

[5] Nomeado EPD, em acumulação com as funções de IN por Despacho do DN da PSP, de 04 de julho de 2022

Nesse contexto, a auditoria e o controlo interno ganham relevância ao promover maior rigor na gestão pública, desenvolvendo soluções, ferramentas, parâmetros e modelos que aumentem a eficiência e a eficácia da gestão.

A função de auditoria e controlo interno segue princípios e normas de conduta, como as Normas Internacionais para a Prática Profissional de Auditoria Interna (AI), estabelecidas pelo The Institute of Internal Auditors (IIA), representado em Portugal pelo Instituto Português de Auditoria Interna (IPAI).

1.2.1. Auditoria Interna

Segundo a definição do IPAI, a AI é "uma atividade independente, de garantia e consultoria, que visa acrescentar valor e melhorar as operações de uma organização. Ela auxilia a organização a atingir os seus objetivos, por meio de uma abordagem sistemática e disciplinada, avaliando e melhorando a eficácia dos processos de gestão de risco, controlo e governação."[6]

Para Silveiro (2020)

> apesar de, habitualmente, a atividade de auditoria ser mais reconhecida quando efetuada por entidades externas à organização (devido ao princípio da independência), a implementação de um órgão de AI competente, eficaz e oportuno, é um dos pilares da estrutura da gestão do risco, que contribuiu para uma gestão eficaz das organizações (p 1).

É relevante salientar que os auditores internos, pela ampla experiência e compreensão aprofundada dos processos e da dinâmica interna da organização, tendem a possuir uma visão mais apurada e detalhada em comparação com os auditores externos.

Essa perspetiva torna a AI uma ferramenta fundamental para acompanhar a implementação e avaliar a eficácia do Sistema de Controlo Interno (SCI), incentivando a constante otimização deste sistema (Silveiro, 2020).

1.2.2. Controlo Interno

O conceito de controlo interno pode ser interpretado de diferentes formas, sendo, por isso, relevante apresentar uma variedade de definições provenientes de diversos autores e instituições, que concluem que o mesmo deve ser entendido como qualquer medida adotada pela gestão com o objetivo de garantir a fiabilidade e integridade da informação, o cumprimento de políticas, planos, procedimentos, leis e regulamentos, bem como a proteção dos ativos (INTOSAI 2024).

---

[6] Obtido em: https://www.ipai.pt/sobre-nos/auditoria-interna-o-que-e/

Por outro lado, numa perspetiva diferente, o Committee of Sponsoring Organizations of the Treadway Commission (2013) define o controlo interno como "um processo realizado pelo conselho de administração de uma entidade, pela gestão e por outros colaboradores, desenhado para proporcionar uma garantia razoável quanto à concretização dos objetivos relacionados com as operações, os relatórios e a conformidade," p. 3).

O IIA (2023) define o controlo interno como "um conjunto de ações, políticas e procedimentos implementados pela gestão para assegurar a integridade e a precisão das informações, o cumprimento de normas e regulamentos, e a proteção dos ativos da organização".[7]

2. A auditoria e controlo interno na PSP

Numa entidade como a PSP, com cerca de 20.000 polícias e pessoal de apoio à atividade operacional, com uma estrutura territorial dispersa por todo o país, e uma das organizações mais complexas no panorama nacional, torna-se necessário e fundamental assegurar a qualidade, credibilidade e independência da estrutura encarregue de efetuar auditoria e controlo interno das suas atividades.

Na PSP as funções de auditoria e controlo interno estão adstritas à IN de forma global, abrangendo todas as áreas de atuação dos Comandos e Serviços, e as centradas na área financeira ou correlacionada ao Departamento de Gestão Financeira (DGF).

2.1. Inspeção Nacional

De acordo com a lei de organização da PSP, artigo 25.º da Lei n.º 53/2007, de 31 de agosto, "compete à Inspeção Nacional exercer o controlo interno nos domínios operacional, administrativo, financeiro e técnico", sendo liderada pelo inspetor nacional e seu regulamento é aprovado pelo ministro da tutela.

O Despacho n.º 14882/2010, de 15 de setembro de 2010 [8], aprova o Regulamento Interno da Inspeção da PSP, que, sob supervisão direta do Diretor Nacional (DN), é responsável pelo controlo interno da PSP, abrangendo as suas competências auditorias e avaliações em áreas como gestão operacional, financeira, administrativa e técnica, assegurando a legalidade, eficácia e eficiência das atividades da PSP.

A IN para o cumprimento das suas competências tem como principais responsabilidades:

---

[7] Obtido em: https://www.theiia.org/en/about-us/about-internal-audit/

[8] Despacho n.º 14882/2010, de 15 de setembro de 2010, do Secretário de Estado Adjunto e da Administração Interna, publicado no DR, 2.ª série N.º 189 — 28 de setembro de 2010.

- Fiscalização e supervisão das atividades internas da PSP, verificando o cumprimento das normas e regulamentos aplicáveis às operações policiais.
- Auditorias e avaliações internas, abrangendo áreas como conformidade com a legislação, eficiência operacional e a conduta dos Polícias e Pessoal de apoio à atividade operacional.
- Controlo disciplinar, atuando em casos de irregularidades, abusos ou desvios de conduta.
- Garantir a legalidade das atividades da PSP, supervisionando a implementação de normas, incluindo aquelas relacionadas com a proteção de dados pessoais.

Constata-se assim, que a IN atua em várias frentes: operações policiais, gestão de recursos humanos, logística e finanças, formação, deontologia e disciplina, e controlo de armas e segurança privada, verificando o cumprimento das normas e procedimentos e propondo melhorias para a qualidade do serviço prestado.

A IN é também responsável pela elaboração de planos anuais de atividades e relatórios, submetidos à aprovação do DN. Os inspetores possuem ampla autonomia para acesso às instalações e documentos da PSP, garantindo um processo de auditoria minucioso e imparcial.

Nos termos do artigo 59.º do Despacho n.º 1168/2024 [9], a IN, além do Inspetor Nacional e do Corpo de Inspetores, é composta por dois serviços:

a) Gabinete de Apoio à Inspeção (GAI): encarregado do apoio administrativo e logístico, gestão documental de auditorias e inspeções, gestão de arquivos, e informação interna e externa;

b) Núcleo de Assessoria Técnica à Inspeção (NATI): responsável por apoiar a atividade da Inspeção com estudos e pareceres nas diversas áreas de intervenção ou conexas, incluindo a proteção de dados pessoais e a colaboração com outras entidades de inspeção do Estado.

2.2. Departamento de Gestão Financeira

O Núcleo de Auditoria Interna (NAI) do DGF, nos termos do artigo 53.º alínea a) do Despacho n.º 1168/2024, sob a supervisão do seu diretor, tem como responsabilidades:

- verificar a conformidade legal dos procedimentos de contratação pública e gestão financeira das unidades da PSP;

[9] Despacho n.º 1168/2024, de 31 de janeiro de 2024, do DN da PSP, publicado no DR, Parte C, 2.ª série, N.º 22 – 31 de janeiro de 2024.

- assegurar a conformidade em contratações de bens, serviços e empreitadas de obras públicas;
- acompanhar a execução financeira de contratos; e
- colaborar com a IN na realização de "auditorias financeiras" para verificar a execução orçamental, elaborando relatórios que indicam irregularidades ou recomendações.
- promover atos relacionados à cobrança coerciva de dívida e execução fiscal.

3. Encarregado de Proteção de Dados

3.1. O Estatuto do EPD

O Estatuto do EPD, conforme definido pelo RGPD, pela Lei n.º 58/2019 e pela Lei n.º 59/2019, pode ser analisado à luz de cada normativo relevando o que cada diploma realça, dando-lhe uma dimensão até aqui inexistente.

O RGPD introduz o conceito do EPD no seu artigo 37.º, como a pessoa responsável por assegurar que as organizações cumprem com a legislação de proteção de dados. O EPD deve ser designado nas seguintes situações:

- Quando o tratamento de dados for realizado por uma autoridade ou organismo público (exceto nos tribunais no exercício da sua função jurisdicional);
- Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistem em operações de tratamento que, pela sua natureza, âmbito e/ou finalidades, exijam um controlo regular e sistemático de dados em larga escala;
- Quando as atividades principais do responsável pelo tratamento ou do subcontratante consistem no tratamento em larga escala de categorias especiais de dados, como dados de saúde ou dados sobre condenações penais.

O EPD pode ser um funcionário da organização ou um consultor externo, devendo ter conhecimentos adequados de legislação e práticas de proteção de dados.

A Lei n.º 58/2019 mantém as disposições do RGPD sobre o EPD, complementando-as com algumas regras específicas no contexto nacional especificando que o EPD deve ter independência funcional dentro da organização, ou seja, não pode receber instruções sobre o exercício das suas funções relativas à proteção de dados pessoais e reportar diretamente ao nível mais elevado da direção.

Esta lei reforça que as organizações devem garantir que o EPD dispõe dos recursos necessários para cumprir as suas funções e reforça igualmente a importância do EPD como

a pessoa responsável pelo contacto entre a organização, os titulares dos dados e as autoridades de controlo, como a CNPD.

A Lei n.º 59/2019, que transpõe para a ordem jurídica nacional a Diretiva 2016/680, também aborda a figura do EPD, estabelecendo que, nos processos relacionados com a investigação e repressão de infrações penais, o EPD desempenha um papel crucial na monitorização da conformidade com as normas de proteção de dados.

O EPD, neste contexto, assegura que os dados pessoais tratados pelas autoridades competentes são utilizados de acordo com os princípios de proteção de dados e que os direitos dos seus titulares são respeitados.

As competências do EPD são reforçadas nesta lei, nomeadamente pela competência, descrita na al. b) do artigo 35.º, para "fiscalizar o cumprimento da presente lei e de outras disposições legais sobre proteção de dados pessoais"

Em termos gerais, o EPD, de acordo com o RGPD e legislação conexa, é o responsável pela supervisão da conformidade da organização com as regras de proteção de dados. O seu papel é fundamental para garantir a transparência, legalidade e segurança no tratamento de dados pessoais, atuando com independência e reportando diretamente à direção da organização.

3.2. Obrigatoriedade e Condições de designação

O artigo 37.º do RGPD estabelece que a nomeação do EPD é obrigatória em todas as autoridades e organismos públicos, excetuando dessa obrigatoriedade os tribunais no exercício de funções jurisdicionais.

A designação de um EPD é também obrigatória se as atividades principais do responsável pelo tratamento dos dados (organização) ou do subcontratante consistirem em operações de tratamento de dados que, pela sua natureza, âmbito e/ou finalidades, exijam um controlo regular e sistemático em larga escala de titulares de dados.

É ainda, obrigatória quando as atividades principais do responsável pelo tratamento ou do subcontratante consistirem no tratamento em larga escala de categorias especiais de dados (como dados de saúde, genéticos, raciais, religiosos, etc.) ou dados relativos a condenações penais e infrações.

A Lei n.º 58/2019, que assegura a execução do RGPD em Portugal, reforça a obrigatoriedade de nomeação do EPD, no seu artigo 9.º, nas condições previstas no RGPD, sem introduzir alterações substanciais. Contudo, clarifica algumas das obrigações das autoridades públicas portuguesas no que diz respeito à nomeação do EPD.

Esta lei enfatiza, no seu artigo 12.º que, para além das entidades privadas obrigadas a nomear o EPD de acordo com os critérios do RGPD, todas as entidades públicas portuguesas devem designar um EPD.

Igual obrigatoriedade consta da Lei n.º 59/2019, no artigo 34.º, daqui resultando uma uniformidade quanto à importância do EPD no ordenamento jurídico no concerne à proteção de dados pessoais.

3.3. Responsabilidades do EPD

As funções do EPD previstas no RGPD, na Lei n.º 58/2019 e na Lei n.º 59/2019, atribuem-lhe como principais responsabilidades:

- Supervisão e monitorização da conformidade da PSP com as regras de proteção de dados pessoais, conforme estabelecido pelo RGPD e legislação conexa.
- Orientação e aconselhamento à direção da PSP e aos seus colaboradores sobre as suas obrigações relativas à proteção de dados.
- Gestão de riscos e realização de avaliações de impacto, sempre que o tratamento de dados puder representar um risco elevado para os direitos dos cidadãos.
- Comunicação com a CNPD em caso de violações ou riscos de conformidade.

4. Síntese conclusiva

Aqui chegados e com o intuito de responder às questões derivadas da questão central deste estudo – "de que forma as práticas de auditoria e controlo interno da Inspeção Nacional da PSP estarão alinhadas com as exigências do RGPD" – apresentamos, a seguir, uma síntese das principais considerações e resultados alcançados, focando-nos na adequação e alinhamento dessas práticas com o quadro normativo vigente.

4.1. Procedimentos de conformidade

Do estudo efetuado resulta que a resposta à QD1 – "De que forma a proteção de dados pessoais é assegurada nas diversas atividades da PSP e que mecanismos e procedimentos garantem a conformidade com o RGPD" – é positiva, pois verificamos que a PSP promove a implementação de medidas estruturais e operacionais que visam proteger os dados pessoais no âmbito das suas atividades, de forma preventiva e contínua.

A PSP assegura a proteção de dados pessoais através de um conjunto de políticas, procedimentos e práticas visando garantir o cumprimento do RGPD e legislação conexa.

Podemos destacar a nomeação de um EPD, que desempenha um papel essencial na monitorização do cumprimento das normas de proteção de dados, aconselhando a direção da PSP, promovendo ações de sensibilização e formação em relação às boas práticas de

tratamento de dados pessoais, e promovendo a realização auditorias periódicas para garantir a conformidade com a legislação.

Através do Departamento de Sistemas de Comunicação e Informação (DSIC) a PSP implementou políticas rigorosas de controlo de acesso aos dados pessoais, assegurando que apenas o pessoal autorizado tem acesso às informações sensíveis. Além disso, foram adotadas medidas de segurança tecnológica, como o uso de encriptação e sistemas de autenticação multifator, para proteger os dados armazenados em sistemas digitais.

Quando é necessário realizar tratamentos de dados pessoais que possam apresentar riscos elevados para os direitos e liberdades dos titulares, é efetuada uma avaliação de impacto. Este processo identifica riscos e define medidas mitigadoras para evitar ou minimizar eventuais violações de dados, procedimentos coordenados pelo DSIC, com intervenção dos departamentos e serviços abrangidos e apoio do EPD.

A PSP tem procedimentos de resposta a incidentes de segurança para a gestão de violações de dados pessoais, que incluem a identificação, contenção e comunicação rápida de eventuais incidentes à CNPD e, quando necessário, aos titulares dos dados, dentro dos prazos legais estabelecidos.

Para garantir que todos os colaboradores estão cientes das suas responsabilidades neste âmbito, a PSP promove formações contínuas sobre a proteção de dados. Estes programas visam não só o cumprimento das obrigações legais, mas também a criação de uma cultura de proteção de dados na instituição.

A PSP realiza verificações sistemáticas às suas práticas de tratamento de dados, com o objetivo de identificar falhas e áreas de melhoria. Estas verificações são conduzidas tanto pelo DSIC, como pelos departamentos responsáveis pelo tratamento e utilização de plataformas que registam dados pessoais, bem como de forma geral pela IN, com acompanhamento do EPD, assegurando uma monitorização constante da conformidade com o RGPD.

Esses mecanismos e procedimentos estão em permanente evolução e demonstram que a PSP adotou e mantém uma abordagem proativa e estruturada para garantir que as suas atividades estão em conformidade com as exigências do RGPD, com o objetivo de proporcionar um elevado nível de proteção aos dados pessoais tratados no âmbito das suas funções e competências para cumprimento da sua principal missão, garantir a segurança pública.

4.2. Prevenção de Violações do RGPD e Conformidade Legal

No que concerne à QD2 – "De que forma as ações de auditoria e controlo interno estão estruturadas e implementadas na PSP para prevenir violações do RGPD, legislação conexa, e assegurar a sua observância" – verificamos que os mecanismos estabelecidos pela PSP para monitorizar, controlar e garantir a conformidade com o RGPD e legislação conexa são diversos.

Apesar de não existir um documento que materializa a estratégia da PSP para o tratamento de dados pessoais, a dispersão de procedimentos não se manifesta como um problema inultrapassável devido essencialmente ao fato do EPD ser cumulativamente o IN e dessa acumulação resultar uma ação de controlo e auditoria que permite à PSP o cumprimento dos normativos legais.

A auditorias internas da PSP são realizadas e/ou supervisionadas pelo EPD e pela IN, com o objetivo de identificar potenciais falhas, áreas de melhoria e assegurar a conformidade com o RGPD e legislação conexa.

As auditorias abrangem, entre outros aspetos, a revisão de procedimentos e políticas de proteção de dados; a verificação da implementação de medidas técnicas e organizativas adequadas; a análise de incidentes anteriores e respostas às violações de dados.

A PSP adotou um sistema de controlo interno contínuo, de algumas plataformas informáticas, como a utilizada pelo Departamento de Investigação Criminal (DIC)[10], através do qual monitoriza o cumprimento das normas de proteção de dados de forma periódica e sistemática. Este sistema envolve a revisão periódica dos procedimentos de tratamento de dados, garantindo que as políticas internas estão constantemente alinhadas com as alterações legislativas ou orientações emitidas pela CNPD.

A realização de avaliações de impacto sobre a proteção de dados (AIPD), especialmente em projetos ou operações que envolvem o tratamento de grande volume de dados pessoais, permite identificar previamente os riscos associados e implementar medidas preventivas adequadas, logo desde a conceção dos projetos.

As auditorias também incluem revisões da gestão de riscos de proteção de dados, onde são estabelecidas medidas de mitigação, como formação, revisão de contratos com subcontratantes, e implementação de tecnologias de segurança.

[10] Plataforma para o Intercâmbio de Informação Criminal (PIIC).

A PSP reconhece que a eficácia das auditorias e do controlo interno depende da consciencialização dos seus colaboradores. Por isso, a formação contínua sobre proteção de dados, destinada a todos os níveis da organização, é uma preocupação que norteia a sua estratégia de formação, estando integrada nos programas de formação de utilização de sistemas informáticos de apoio à atividade policial, como o Sistema Estratégico de Informação (SEI), na gestão das reclamações, etc.

Sempre que as auditorias ou o controlo interno identificam falhas no cumprimento do RGPD, a PSP implementa ações corretivas imediatas. Essas ações podem incluir a revisão de políticas, a introdução de novas medidas de segurança, ou até mesmo sanções disciplinares em casos de negligência, se outros procedimentos legais mais graves não se justificarem, em caso de dolo.

A PSP mantém uma colaboração próxima com a CNPD, reportando qualquer violação de dados dentro dos prazos estabelecidos e participando ativamente em investigações ou inspeções conduzidas pela autoridade de controlo. Esta cooperação garante que as suas práticas de auditoria e controlo interno estão continuamente alinhadas com as exigências do RGPD e da legislação conexa, tanto a nível nacional como europeu.

As ações de auditoria e controlo interno da PSP estão estruturadas de forma sistemática e proativa para prevenir violações do RGPD e garantir a observância das legislações conexas. Através da implementação de auditorias regulares, monitorização contínua, formação de colaboradores e revisão de procedimentos, a PSP assegura que as suas práticas estão alinhadas com os mais elevados padrões de proteção de dados, cumprindo as exigências do RGPD e mitigando o risco de infrações.

4.3. Compatibilidade das Competências do EPD e da IN

Para analisar a compatibilidade entre as competências da IN e do EPD, respondendo dessa forma à QD3 – “de que forma as competências da IN são ou não compatíveis com as competências do EPD” – é necessário entender as suas funções e responsabilidades específicas dentro da PSP. Só dessa forma as competências da IN e do EPD na PSP podem ser vistas como complementares, mas com responsabilidades distintas e bem definidas.

No entanto, pode haver áreas de interseção, especialmente no que diz respeito ao controlo e supervisão das práticas de tratamento de dados pessoais.

As competências podem sobrepor-se em certos aspetos, como a supervisão da conformidade com a legislação em relação à proteção de dados pessoais, mas têm focos de atuação diferentes, podendo potenciar situações de risco de incompatibilidade.

Da análise das funções de cada um, podemos de forma sucinta referir as seguintes:

4.3.1. Áreas de atuação compatíveis

- *Fiscalização e conformidade legal*: A IN e EPD estão envolvidas em assegurar que a PSP esteja em conformidade com a legislação, incluindo o RGPD e legislação conexa. A IN pode fiscalizar a conformidade global da PSP com a legislação, enquanto o EPD foca-se especificamente nas questões de proteção de dados.
- *Controlo interno*: Tanto a IN quanto o EPD podem realizar auditorias ou avaliações relacionadas com a proteção de dados, embora a IN tenha uma função mais abrangente, enquanto o EPD se concentra exclusivamente nas questões de privacidade e segurança dos dados pessoais.
- *Segurança e gestão de riscos*: O EPD atua diretamente na gestão de riscos relacionados com o tratamento de dados pessoais, o que pode ser complementado pela fiscalização mais ampla da IN em termos de segurança e legalidade das operações da PSP.

4.3.2. Áreas de atuação diferenciada

- *Foco principal*: O EPD tem uma competência especializada e exclusiva no que diz respeito à proteção de dados pessoais e à conformidade com o RGPD. A IN, por outro lado, tem um foco mais amplo e atua em várias áreas operacionais e legais da PSP.
- *Papel consultivo do EPD*: O EPD tem um papel proeminente de aconselhamento e formação sobre questões específicas de proteção de dados, o que não se aplica diretamente à IN. O EPD orienta a PSP no desenvolvimento de boas práticas, enquanto a IN se foca mais na verificação do cumprimento das normas, sem prejuízo de propor ações de melhoria. No âmbito da Lei n.º 59/2019, as funções do EPD são acrescidas em especial pela obrigação de fiscalização do cumprimento da mesma.
- *Competência disciplinar da IN*: A IN tem poder para atuar diretamente em casos de má conduta ou incumprimento de normas gerais dentro da PSP, tem o dever de cumprir os normativos legais no âmbito do estatuto disciplinar da PSP, propondo o procedimento de natureza disciplinar adequado, enquanto o EPD apenas reporta questões relativas a proteção de dados, podendo fazer recomendações, mas, não tem autoridade disciplinar.

4.4. Riscos de Incompatibilidade

- *Potencial sobreposição*: Em situações de auditoria ou controlo, pode haver uma sobreposição de funções, já que tanto a IN quanto o EPD podem estar envolvidos na fiscalização ou auditoria de conformidade com as normas legais relativas a proteção de dados. A coordenação clara entre as duas funções é essencial para evitar duplicidade de esforços.
- *Independência do EPD*: O EPD deve atuar de forma independente, conforme estipulado pelo RGPD. Embora a IN tenha autoridade sobre várias áreas da PSP, o EPD não pode estar sujeito a interferências hierárquicas que comprometam sua independência na supervisão de proteção de dados pessoais, considerando por exemplo a obrigação legal de comunicação obrigatória de eventual violação das normas legais relativas a proteção de dados à CNPD.

4.5. Medidas de mitigação e eliminação de riscos de incompatibilidade

Para mitigar os riscos de incompatibilidade entre as competências da IN e do EPD na PSP, é essencial implementar medidas que promovam a coordenação, a clareza de funções e a comunicação entre as duas entidades, o que no caso em estudo é de difícil execução em virtude do Inspetor Nacional acumular a função de EPD, nomeadamente:

- É necessária uma definição clara de funções e responsabilidades, estabelecendo normas internas que clarifiquem as competências da IN e do EPD, delimitando claramente as áreas de atuação de cada um. Este fator é tão mais relevante em virtude do dirigente máximo da IN ser o Inspetor Nacional, e simultaneamente EPD.
- Garantir que a IN se concentre nas auditorias gerais da PSP, enquanto o EPD se foque exclusivamente na proteção de dados pessoais e conformidade com o RGPD.
- Desenvolvimento de protocolos de colaboração entre a IN e o EPD, delineando como as duas entidades devem trabalhar em conjunto, compartilhando informações relevantes sem comprometer a independência do EPD.
- Realização de reuniões periódicas entre a IN e o EPD para discutir áreas de potencial sobreposição e garantir que ambas as partes compreendem as atividades e prioridades uma da outra.
- Planeamento e execução de auditorias coordenadas, sempre que adequado, para evitar duplicidade de esforços. A IN e o EPD devem coordenar-se para que as

auditorias realizadas por cada uma das entidades sejam complementares e não redundantes.

- Criar calendários de auditorias compartilhados para garantir que a IN e o EPD realizem as suas auditorias de maneira integrada, respeitando os diferentes focos de cada entidade.
- Promover ações de formação conjuntas que envolvam tanto os responsáveis pela IN quanto o EPD, focadas em esclarecer as suas funções e a importância da colaboração na prevenção de conflitos ou sobreposições.
- Realizar sessões de sensibilização para os colaboradores da PSP, de modo a clarificar os papéis da IN e do EPD, prevenindo mal-entendidos ou confusões sobre as suas responsabilidades.
- Estabelecimento de canais de comunicação formais entre a IN e o EPD para troca de informações e partilha de relatórios de auditoria e revisões, garantindo que ambos têm acesso a dados relevantes sem comprometer a independência do EPD.
- Criar um sistema de relatórios conjuntos para assuntos que envolvam tanto a fiscalização geral quanto a proteção de dados, permitindo que ambas as partes participem na avaliação de riscos e de conformidade.
- Implementação de um sistema de revisão contínua das interações e da eficácia das medidas de colaboração entre a IN e o EPD, com ajustes sempre que forem identificadas áreas de incompatibilidade ou sobreposição.
- Avaliações de impacto internas sobre a atuação das duas entidades para identificar eventuais riscos de incompatibilidade e assegurar que as suas competências continuem complementares ao longo do tempo.
- Reforçar, por meio de políticas internas claras, a independência do EPD em todas as suas funções, assegurando que as auditorias ou recomendações da IN não interfiram ou limitem as decisões e ações do EPD.
- Garantir que o EPD não seja subordinado direta ou indiretamente à IN, para evitar conflitos de interesse ou influência indevida nas suas decisões, situação que no tempo do estudo não se coloca pela acumulação de funções do Inspetor Nacional com as de EPD.
- Criar uma comissão interna de supervisão que inclua membros da IN, do DSIC, do Gabinete de Assuntos Jurídicos (GAJ) e o EPD, com o objetivo de gerir conflitos

de competência e promover uma cooperação eficiente em áreas de interseção de responsabilidades.

As medidas elencadas decorrem do estudo efetuado e são orientadoras, visando garantir que as competências da IN e do EPD sejam respeitadas e bem coordenadas, evitando sobreposições e garantindo a conformidade tanto com a legislação geral como com o RGPD, ao mesmo tempo que preservam a eficiência operacional da PSP.

As competências da IN e do EPD podem ser compatíveis se forem bem coordenadas e respeitadas as áreas de atuação distintas de cada entidade. O EPD tem uma função especializada e independente na proteção de dados pessoais, enquanto a IN tem um papel mais abrangente de controlo e fiscalização de diversas atividades da PSP.

Desde que sejam respeitadas as suas especificidades e independência, as funções podem complementar-se para garantir uma conformidade abrangente com a legislação, tanto no âmbito geral como no específico da proteção de dados pessoais.

Conclusão

Os desafios atuais da proteção de dados pessoais na PSP à luz do RGPD e da legislação conexa, como a Lei n.º 58/2019 e Lei n.º 59/2019, dão uma dimensão acrescida às atividades de AI. O estudo centrou-se na análise das práticas de auditoria e controlo interno implementadas pela PSP, com o objetivo de assegurar o cumprimento das exigências legais, proteger os direitos dos cidadãos e preservar a confiança pública na instituição.

Ao longo da investigação, foi possível observar que, embora a PSP tenha dado passos significativos para alinhar suas operações com as exigências do RGPD, persistem desafios estruturais e operacionais que requerem atenção.

A criação e nomeação do EPD e a existência de uma IN com competência em auditoria e controlo interno são pontos positivos no esforço de conformidade, mas a sobreposição de funções entre estas duas entidades levanta questões sobre a eficácia e independência na supervisão do tratamento dos dados pessoais.

O estudo identificou que, apesar da ausência de um documento centralizador de estratégia de proteção de dados, a PSP adota uma abordagem dispersa, mas funcional, que envolve a implementação de políticas de acesso restrito, a utilização de tecnologias de segurança avançadas e a realização de verificações periódicas para monitorizar o cumprimento das normas. No entanto, essas práticas ainda carecem de maior sistematização e de uma cultura mais enraizada de proteção de dados transversal a todos os níveis da instituição.

Relativamente à auditoria e controlo interno, a investigação revelou que os mecanismos atualmente em vigor, embora eficazes em muitas áreas, podem ser otimizados. A acumulação das funções do Inspetor Nacional e do EPD, embora promova uma coordenação centralizada, pode comprometer a independência do EPD e limitar a fiscalização isenta das práticas de proteção de dados. Esta sobreposição é um dos principais riscos identificados, uma vez que o RGPD exige que o EPD atue de forma independente, isenta e imparcial.

A análise das práticas de auditoria revelou também que, apesar de existirem mecanismos de monitorização contínua e uma política de resposta a incidentes de segurança, a PSP deve reforçar suas avaliações de impacto e revisões periódicas de políticas internas. Isso permitirá uma resposta mais ágil e eficaz às constantes mudanças no cenário legislativo e tecnológico.

Propostas para o futuro foram elaboradas com base nos resultados alcançados. Em primeiro lugar, é essencial a definição clara e formal das competências e responsabilidades da IN e do EPD, estabelecendo protocolos de colaboração que assegurem a complementaridade e evitem conflitos de funções. Um plano estruturado de coordenação entre estas duas entidades permitirá que cada uma cumpra eficazmente o seu papel, sem comprometer a independência do EPD.

Adicionalmente, recomenda-se a criação de um documento estratégico que centralize as políticas e procedimentos de proteção de dados da PSP, promovendo uma visão unificada e facilitando a formação contínua de todo o efetivo. Este documento será fundamental para uma boa gestão de todas as bases de dados existentes, garantindo os direitos dos titulares dos dados pessoais ali tratados, nomeadamente o acesso, retificação e apagamento.

A implementação de programas regulares de sensibilização e formação sobre o RGPD é igualmente crucial para garantir que todos os polícias e pessoal de apoio à atividade operacional compreendam a importância da proteção de dados pessoais e atuem em conformidade com as melhores práticas.

A PSP também deve investir na modernização das suas tecnologias de segurança, com foco na proteção de dados, assegurando que as informações pessoais dos cidadãos e dos seus recursos humanos estão devidamente encriptadas e protegidas contra acessos não autorizados ou ataques cibernéticos.

Paralelamente, a PSP deve reforçar os seus mecanismos de resposta a incidentes, garantindo uma comunicação eficiente com a CNPD e com os titulares dos dados, conforme exigido pelo RGPD e legislação conexa.

Finalmente, a criação de uma comissão interna de supervisão, composta por membros da IN, do Departamento de Sistemas de Informação e Comunicação (DSIC), do Gabinete de Assuntos Jurídicos (GAJ) e do EPD, pode ajudar a gerir conflitos de competências e promover uma cooperação eficiente em áreas de interseção. Essa comissão teria o papel de avaliar, de forma contínua, as interações entre as diferentes unidades operacionais e de apoio e garantir que as competências da IN e do EPD permanecem complementares e eficazes ao longo do tempo.

Em síntese, conclui-se que a PSP tem demonstrado esforços relevantes para alinhar suas práticas às exigências do RGPD e legislação conexa, mas ainda enfrenta desafios consideráveis. A otimização dos mecanismos de auditoria e controlo interno, a clarificação das competências do EPD e da IN, bem como a criação de uma cultura institucional sólida

em torno da proteção de dados, são elementos cruciais para o futuro da conformidade com o RGPD. Somente através da implementação dessas medidas será possível garantir a proteção dos direitos dos cidadãos, reforçar a confiança pública e promover uma PSP mais transparente, eficaz e responsável na era digital.

Portanto, o papel do EPD é essencial na PSP para garantir que os dados pessoais dos cidadãos sejam protegidos de forma adequada, alinhando-se às obrigações impostas pelo RGPD e evitando possíveis abusos ou desvios na utilização dos dados. A nomeação de um EPD capacitado e independente reforça a confiança dos cidadãos na instituição, assegurando que a sua privacidade e direitos sejam devidamente salvaguardados.

Bibliografia

Referências:

Andrade, R. R. (2020, dezembro). Da responsabilidade do encarregado de proteção de dados. *Fórum de Proteção de Dados*, *7*, 24–43.

Arvelos, S. M. G. (2023). *Proteção de dados pessoais da PSP: Que desafios?* [Report]. https://comum.rcaap.pt/handle/10400.26/45942

A Era Digital e os Direitos: O Que Mudou com as Novas Regulamentações da União Europeia - DIGITAL SPRINT. (2023, outubro 21).

https://digitalsprint.pt/a-era-digital-e-os-direitos-o-que-mudou-com-as-novas-regulamentacoes-da-uniao-europeia/

Auditoria Interna, o que é ? (sem data). Obtido 16 de setembro de 2024, de https://www.ipai.pt/sobre-nos/auditoria-interna-o-que-e/

Clemente, P. (2006), A Polícia em Portugal, Instituto Nacional de Administração

Carta dos Direitos Fundamentais da UE. (2012, julho 20). European Union Agency for Fundamental Rights. http://fra.europa.eu/pt/eu-charter

Comissão Europeia. (2020). *Plano de Ação para a Educação Digital 2021-2027*. https://digital.dge.mec.pt/sites/default/files/documents/2022/176-669bb450baf49f365baf254c7d1f2ac8.pdf

Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 01 julho 2015 Semestral "O Novo Quadro Legal Europeu" [Em linha]. Lisboa CNPD. [Consult.07/02/2018]. Disponível em:

https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-1.html

Constituição da República Portuguesa—CRP | DR. (sem data). Obtido 14 de setembro de 2024, de https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775

Correia, P. M. A. R., & Jesus, I. O. A. de. (2014). A proteção de dados pessoais no Espaço de Liberdade, de Segurança e de Justiça da União Europeia. *Revista Brasileira de Segurança Pública*, *8*(2), Artigo 2. https://doi.org/10.31060/rbsp.2014.v8.n2.385

Funções do EPD. (sem data). *Portal do DPO - Encarregado de Proteção de Dados*. Obtido 11 de abril de 2024, de https://www.portaldodpo.pt/funcoes-do-dpo/

Institute of Internal Auditors. (2023). https://www.theiia.org/en/about-us/about-internal-audit/

IIA - Institute of Internal Auditors The Impact of Globalization on Internal Auditors: The Evolution of Internal Auditing (2002). https://na.theiia.org/about-us/Public%20Documents/Sawyer_Award_2002.pdf Consultado em maio 2024.

IIA - Institute of Internal Auditors (2017). International standards for the professional practice of internal auditing. https://na.theiia.org/standardsguidance/Public Documents/IPPF-Standards-2017.pdf

IIA - Institute of Internal Auditors – Documento de Exposição – Três Linhas de Defesa (junho 2019): https://na.theiia.org/translations/PublicDocuments/3LOD-IIA-Exposure-Document-Portuguese.pdf

IIA - Institute of Internal Auditors - ONRISK A Guide to Understanding, Aligning, And Optimizing Risk 2020. http://contentz.mkt5790.com/lp/2842/275148/OnRisk-2020-Report_0.pdf Consultado em agosto 2024.

IIA Portugal - IPAI – O Modelo das Três Linhas do IIA – uma atualização das Três Linhas de Defesa (12/08/2020):

https://www.ipai.pt/fotos/gca/o_modelo_das_tres_linhas_do_iia_v_jlp_3ago2020_v lcs_final_12ago2020_1597332421.pdf

INTOSAI. (2024). https://www.intosai.org/what-we-do/professional-standards/sc-subcommittees.html

Moreira, T. F. M. (2018). *O impacto do regulamento geral de proteção de dados nas organizações: Um novo paradigma* [masterThesis]. https://comum.rcaap.pt/handle/10400.26/23465

Saldanha, Nuno (2019) *RGPD Guia para uma Auditoria de Conformidade* - Dados Privacidade, Implementação, Controlo, Compliance, FCA - Editora de informática Lda. Lisboa, 1ªEdição.

Teves, D. M. (2019). *A proteção de dados pessoais: O novo paradigma jurídico*.

Teixeira, J. M., Revista Hits, artigo de opinião - Auditoria Internado Compliance à Criação de Valor https://www.pwc.pt/pt/hits/artigos-opiniao/jose-teixeira.html, consultado em junho 2024.

Tic.Gov.Pt. (2023). *Estratégias*. https://www.tic.gov.pt/estrategias/estrategia-2021-2026

Shinde, B. (2021, dezembro 1). *Artificial Intelligence Adoption in Internal Audit Processes*. ISACA.https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-40/artificial-intelligence-adoption-in-internal-audit-processes

Silveiro, P. R. P. (2020). *Modelo de auditoria Interna como apoio à decisão na Guarda Nacional Republicana*. https://comum.rcaap.pt/handle/10400.26/33160

Vaz, A. R. (2018). *O Regulamento Geral de Proteção de Dados: Desafios e Impactos* Universidade Coimbra, https://estudogeral.uc.pt/bitstream/10316/85758/1/Disserta%C3%A7%C3%A3o.pdf

Veiga, A. S. P. G. (2020). *Proteção de dados: O direito à privacidade na era digital.* [Universidade Autónoma de Lisboa]. https://repositorio.ual.pt/handle/11144/5046

Veiga, P. (2022, fevereiro 17). *Desafios de Segurança no Mundo Digital*. Fundação Francisco Manuel dos Santos.

https://ffms.pt/pt-pt/atualmentes/desafios-de-seguranca-no-mundo-digital

World Economic Forum. (2024, março 14). *11 technology milestones that changed our lives*. World Economic Forum. https://www.weforum.org/agenda/2024/03/11-technology-milestones-ai-quantum-computing-vr/

Zambelli, R. (2023, fevereiro 6). Auditoria interna: O que é e qual a sua importância para empresas. *Blog | Checklist Fácil*. https://blog-pt.checklistfacil.com/auditoria-interna/

Legislação:

Comissão Nacional de Proteção de Dados - Fórum de Proteção de dados nº 01 julho 2015 Semestral "O Novo Quadro Legal Europeu" [Em linha]. Lisboa CNPD. [Consult.07/02/2018]. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-1.html

Grupo de Trabalho do Artigo 29.o. (2016). Orientações sobre os encarregados da proteção de dados (EPD). WP 243 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=612048

Lei n.º 43/2004, de 18 agosto - Lei de organização e funcionamento da Comissão Nacional de Proteção de Dados – Republicada pela Lei n.º 58/2019 de 08 agosto https://dre.pt/dre/detalhe/lei/43-2004-123815982

Lei n.º 53/2007, 31 agosto – Aprova a orgânica da Polícia de Segurança Pública https://dre.pt/dre/detalhe/lei/53-2007-641142

Lei n.º 58/2019, de 28 agosto – 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 https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Lei n.º 59/2019 de 8 de agosto, aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT Consultado em julho de 2024.

Regulamento (UE) 2016/679 - RGPD https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:32016R0679