INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

MODERNIZAÇÃO DO BILHETE DE IDENTIDADE POLICIAL: CONTRIBUTO PARA A CRIAÇÃO DO CARTÃO DIGITAL NA PSP

Auditor

João Paulo Pereira Martelo

Lisboa, 03 de outubro de 2025

Resumo

O avanço das tecnologias de identificação digital, a desmaterialização de documentos e a crescente aposta do Estado português e da União Europeia na Governação Digital, levou à criação de normas jurídicas que legitimam o reconhecimento mútuo da assinatura eletrónica qualificada através de serviços de confiança para autenticação e transações entre Estados Membros. O Estado permite a assinatura eletrónica qualificada, através do cartão de cidadão e chave móvel digital, mas, em termos legais, não permite à grande percentagem dos policias associar os atributos profissionais à assinatura qualificada; apenas uma pequena percentagem o consegue, atendendo às funções e cargos desempenhados.

Nesta linha de pensamento, apoiada na capacidade de abertura que as organizações detêm para a inovação tecnológica, torna pertinente a possibilidade de estudar a hipótese da criação de um cartão policial digital para a Polícia de Segurança Pública. Foi de nosso particular interesse promover o enquadramento teórico dos conceitos da assinatura digital qualificada associado à garantia jurídica da assinatura eletrónica qualificada com os atributos profissionais inerentes, concentrando depois o propósito no contexto atual da Polícia de Segurança Pública.

Palavras-chave: Assinatura eletrónica, Atributos profissionais, Cartão digital, Polícia de Segurança Pública

Abstract

The advancement of digital identification technologies, the dematerialization of documents, and the growing commitment of the Portuguese State and the European Union to Digital Governance have led to the creation of legal norms that legitimize the mutual recognition of qualified electronic signatures through trust services for authentication and transactions between Member States. The State allows the use of qualified electronic signatures through the citizen card and digital mobile key, however, from a legal standpoint, it does not allow a large percentage of police officers to associate professional attributes with the qualified signature; only a small percentage are able to do so in accordance with the functions and roles they perform.

In this line of thought, supported by the openness that organizations have to technological innovation, the hypothesis of studying the possibility of creating a digital police card for the Public Security Police becomes pertinent. We were particularly interested in promoting the theoretical framework of the concepts of qualified digital signatures associated with the legal guarantee of the qualified electronic signature and the associated professional attributes, thus focusing our purpose on the current context of the Public Security Police.

Keywords: Electronic signature, Professional attributes, Digital card, Public Security Police.

Agradecimentos

Índice

Resumo ii

Abstrat iii

1. Introdução 1

2. Enquadramento Teórico e Estado da Arte: A Identidade Digital e os Desafios da Modernização na Atividade Policial 3

2.1. O Paradigma da Governança Digital na Modernização do Estado 3

2.2. A Construção da Infraestrutura de Confiança Digital 5

2.2.1. O Alicerce: A Identidade Eletrónica do Cidadão 6

2.2.2. A Garantia Jurídica: O Regulamento eIDAS e a Assinatura Eletrónica Qualificada (AEQ) 9

2.2.3. A Lacuna Teórica e Prática: A Ausência da Identidade Profissional 11

2.3. Interoperabilidade e os Desafios Sociotécnicos na Cultura Policial 13

2.4. O Acto Policial Digital: Implicações, Validade e a Fronteira da Prova 15

3. Método 16

4. Perspetivas 17

5. Discussão e Conclusão 21

Referências bibliográficas 24

Anexo 1 40

1. Introdução

A transformação digital é uma prioridade estratégica da União Europeia (UE) e de todos os países que a constituem. Em Portugal, verifica-se uma crescente competitividade no mercado das Tecnologias de Informação e Comunicação (TIC) e uma tendencial transformação digital da Administração Pública (AP), incluindo-se aí a Polícia de Segurança Pública (PSP). A adoção de ferramentas tecnológicas tem vindo a transformar as práticas policiais, verificando-se uma crescente substituição dos documentos físicos, por sistemas digitais integrados, promovendo maior eficiência e governação digital (Rito et al., 2019).

Esta evolução tecnológica e digital resulta na otimização de recursos, diminuindo a burocracia, robustecendo a transparência, promovendo maior responsabilidade, bem como uma maior interoperabilidade dentro da AP, levando a uma crescente satisfação dos cidadãos e empresas, na obtenção de serviços céleres pelas instituições públicas (Carmo et al., 2025).

Uma instituição como a PSP deverá, obrigatoriamente, acompanhar a velocidade do quadro da interoperabilidade permitido pelas transformações tecnológicas (Pereira, 2017), como sucede no envio do expediente criminal, através da interoperabilidade entre sistemas da PSP e do Ministério Público (MP) [(Canelas, 2017)]. No entanto, a gradual eliminação do suporte físico do expediente criminal em detrimento do suporte digital pelo MP (MP, 2025) e Tribunais[1] e a consequente tramitação eletrónica dos processos judiciais[2], exige a adoção da Assinatura Eletrónica Qualificada (AEQ) em todos os atos processuais criminais/administrativos produzidos pela PSP.

Salienta-se que uma das evoluções tecnológicas de maior impacto no nosso país, na sequência da estratégia de modernização da AP, foi a criação do Cartão de Cidadão (CC) e a inclusão da AEQ (Rito, 2018). Contudo constata-se que, em regra, a assinatura eletrónica, via CC ou Chave Móvel Digital (CMD) não contempla os atributos profissionais necessários para validar, juridicamente, os atos praticados pela esmagadora maioria dos polícias, enquanto Órgão de Polícia Criminal (OPC), cf. art. 1.º al. c) do Código Processo Penal (CPP). Atualmente, apenas aos dirigentes da PSP, cuja nomeação tenha sido publicada em Diário da República Eletrónico (DRE), podem solicitar a certificação dos seus atributos públicos, através do Sistema de Certificação de Atributos Profissionais (SCAP) [(art. 11.º e

[1] Tramitação eletrónica processos entre MP e Tribunais
[2] Autorização para PSP adquirir software de interoperabilidade de apoio à atividade Tribunais e do sistema estratégico de informação da PSP.

12.º da Portaria n.º 73/2018, de 12 de março)], comprovando o cargo que exercem, para posterior autenticação e assinatura através do CC ou da CMD (n.º 10 do Decreto-Lei n.º 83/2016, de 16 de dezembro).

É alicerçado nas virtudes acima identificadas que reside o contexto geral do problema em investigação, nesta transição do formato físico-documental para o digital, nomeadamente com a implementação de assinatura qualificada com atributos profissionais para todos os polícias da PSP, com recurso à AEQ, contendo os atributos profissionais.

Os constrangimentos e desafios para a PSP, na continuação da aposta na digitalização dos processos administrativos (PA) e operacionais, reside, essencialmente, no facto da maioria dos polícias não possuírem uma assinatura eletrónica que contenha os atributos profissionais. Pelo exposto, estamos perante constrangimentos e desafios técnico-legais causados pela dificuldade na autenticação de documentos elaborados pela PSP, na qualidade de Autoridade de Polícia Criminal (APC) [(art. 1.º al. d) do CPP)] ou de OPC.

Em Portugal, a Resolução de Conselho Ministros n.º 98/2020, de 13 de novembro – Estratégia Portugal 2030 - reforça o objetivo de impulsionar a modernização e digitalização da AP e simplificação dos PA. A Estratégia para a Transformação da Digital da Administração Pública (ETDAD) 2021 – 2026, cujo objetivo é tornar os serviços públicos mais próximos do cidadão e empresas, disponibilizando serviços simples, integrados e inclusivos, de forma mais eficiente e transparente, através do potencial transformador das tecnologias digitais e da utilização estratégica dos dados, fato que é reforçado pela Lei n.º 24-C/2022, de 30 de dezembro – Lei das Grandes Opções para o quadriénio 2022-2026, mais concretamente no que se refere às linhas estratégicas para a segurança interna, evidenciando a relevância do investimento na modernização tecnológica das forças e serviços de segurança.

Neste contexto de modernidade e transformação digital da PSP, a Estratégia da PSP 2025-2027 (EPSP 25/27) evidencia, no seu eixo estratégico Inovação e Desenvolvimento que, o impulsor tecnológico da PSP é o Plano Estratégico dos Sistemas e Informações (PESI2), salientando que a sua execução é crucial para impulsionar o processo transformacional-digital da PSP.

Após análise exploratória do tema e tendo em conta o progresso das tecnologias de identificação digital, a desmaterialização de processos e a tendencial aposta de Portugal nas soluções do governo eletrónico (Rito et al., 2019), conclui-se que a PSP tem de criar as condições necessárias para uma modernização digital.

Assim, definiu-se como Pergunta de Partida para a realização deste trabalho: De que forma a introdução de uma identidade digital profissional com assinatura qualificada redefine os conceitos de autoridade, responsabilidade e legitimidade processual na cultura organizacional da PSP? A escolha do tema deste trabalho enquadra-se na lista de temas para a realização do Trabalho Individual Final, definido como orientação para o VI Curso de Comando e Direção Policial do Instituto Superior de Ciências Policiais e Segurança Interna, sobre a temática do ponto VII "Tecnologias de Segurança", 1. A Segurança Tecnológica na PSP. A pertinência da investigação decorre da necessidade de clarificar o objeto, carecendo de explicação ou, de um entendimento mais profundo (Fortin, 2009).

Encontrado o ponto de partida, que podemos definir como fio condutor do trabalho (Quivy & Campenhoudt, 2005), torna-se essencial estruturar o percurso metodológico, orientado pelos objetivos gerais e específicos, de forma a garantir a construção de novo conhecimento e a evitar dispersões por temáticas paralelas. O objetivo geral deste estudo é analisar a viabilidade jurídica, tecnológica e operacional da implementação de um cartão policial com AEQ na PSP. Os objetivos específicos: i) identificar o enquadramento legal nacional e europeu da certificação de atributos profissionais; ii) analisar diferenças entre o enquadramento legal nacional e europeu; iii) mapear requisitos tecnológicos e de infraestruturas necessárias para a emissão e utilização do cartão policial digital; iv) verificar casos de forças policiais europeias que já tenham implementadas soluções semelhantes; v) propor um modelo conceptual para a implementação do cartão policial digital na PSP.

O presente trabalho inicia-se com uma breve revisão da literatura, na senda do conceito da identificação digital, abordando a infraestrutura, alicerce e garantia jurídica da AEQ, CMD e assinatura qualificada com os atributos profissionais. Seguidamente será efetuada uma breve reflexão sobre interoperabilidade e o ato policial digital. Por fim, concentraremos as atenções na assinatura eletrónica associada ao cartão policial digital de forças policiais de outros países europeus, que o utilizam, refletindo sobre o quadro do atual bilhete de identidade da PSP, procurando assim, dar respostas à pergunta de partida e às respetivas perguntas derivadas que adiante abordaremos.

2. Enquadramento Teórico e Estado da Arte: A Identidade Digital e os Desafios da Modernização na Atividade Policial

2.1. O Paradigma da Governança Digital na Modernização do Estado

A evolução exponencial das tecnologias e a sua aplicação deu origem à Governação Digital (GD), conceito que se alargou desde o início do emprego das TIC na AP, até à atualidade, em que o binómio informações/tecnologia impulsionam a sociedade da informação (Gil-Garcia et al., 2018). A utilização das TIC pela GD e a disseminação da informação digital por toda a sociedade proporcionou governos mais eficientes, eficazes, transparentes, reforçando a cidadania (Cardoso, 2018; Carneiro, 2019; Gil-Garcia et al., 2018; Rito et al., 2019). O pilar central da modernização administrativa é a interoperabilidade e a informação, originando a promoção de valores, como a abertura e a participação, com foco no cidadão e no princípio *only-one*, visando criar uma AP apta a responder a uma sociedade em constante mudança (Almeida, 2019; Cardoso, 2018; Parisopoulos, et al., 2007; Pena, 2020; Soares, 2022;).

A estratégia digital da UE centra-se, primordialmente, nas pessoas, gerando também oportunidades para as empresas. A transição digital da UE, assenta em três pilares (CE, 2024): tecnologia ao serviço dos cidadãos; economia digital justa e competitiva; sociedade aberta, democrática e sustentável. A UE criou o Programa Europa Digital (CE, 2021), para promover domínios prioritários como a identidade digital e as infraestruturas públicas. Já a estratégia digital portuguesa (Governo português, 2024) pretende tornar a AP mais digital, apostando no potencial transformacional das tecnologias digitais, através de serviços integrados, mais eficientes e inclusivos para cidadãos e empresa. Obviamente estas transformações na AP proporcionaram maior interação e colaboração com outras instituições públicas e privadas, bem como com os cidadãos, colocando, assim, em causa o modo tradicional de administração (Gil-Garcia et al., 2018). A Nova Gestão Pública (*New Public Management*) introduziu reformas, novas lógicas de gestão importadas do sector privado, alargando os serviços públicos a cidadãos e empresas, visando redução de despesas, uma AP mais eficiente e políticas públicas mais eficazes (Almeida, 2019; Iacovino et al., 2017; Morgado, 2013; Parisopoulos, et al., 2007).

A evolução exponencial das tecnologias e sua aplicabilidade deu origem à GD (Gil-Garcia et al., 2018). Em 2012, Cardoso refere que as plataformas digitais promovem uma AP centrada no cidadão, mais célere, eficiente, eficaz, proporcionando um acesso mais simples, favorecendo tanto os cidadãos (*Government to Citizens*), como empresas (*Government to Business*) e, por fim a AP (*Government to Government*).

A AP deixou de ser uma organização fechada, com uma estrutura hierárquica rígida (modelo *top-down*), no qual os decisores concentravam-se em traçar objetivos e monitorizar a sua aplicação, unicamente centravam em criar objetivos, controlando a sua implementação

e não dando ênfase ao mérito ou a qualidade do serviço prestado. Em seu lugar, tem vindo a consolidar-se uma estrutura híbrida, que conjuga a autoridade formal através de mecanismos mais participativos e orientados à obtenção de resultados, valorizando a eficiência, a transparência e a satisfação dos cidadãos. (Emery & Giauque, 2014; Souza, 2018; Ongaro, 2015), ajustando-se às necessidades de sociedades e cidades modernas, impondo inovação e competência ao serviço público (Cardoso, 2018; Mozzicafreddo, 2017). Em 2012, Cardoso refere que "a administração muda de um modelo vertical, meramente burocrático, tipo *top-down*, para uma administração mais horizontal onde as diretrizes são a cooperação e a interação" (p. 16).

O Governo português, em 2006, criou o programa Simplex, suportado pela Plataforma de Interoperabilidade da Administração Pública (iAP) [(AMA, 2015)], visando a modernização e desburocratização da AP, criando serviços centrados no cidadão e empresas, permitindo a troca segura de dados entre os diversos organismos públicos, acelerando processos, reforçando a transparência com a disponibilidades de dados abertos e o reforço da responsabilidade na prestação de contas (Almeida & Ferreira, 2019; Magalhães et al., 2025).

2.2. A Construção da Infraestrutura de Confiança Digital

Em Portugal, o ecossistema tecnológico que permite a identidade eletrónica (eID) dos cidadãos, são o CC e a CMD, assente no Sistema de Certificação Eletrónica do Estado (SCEE), responsável pela Infraestrutura de Chaves Públicas (PKI), englobando um conjunto de tecnologias de hardware e software em sistemas interoperáveis entre órgãos públicos e privados (Correia, 2024; Pena, 2020). O CC contém dois certificados (ARTE, 2025a), um para autenticação (ARTE, 2025b), outro para a AEQ (ARTE, 2025c); a CMD possibilita a autenticação (ARTE, 2025d) e a AEQ (ARTE, 2025e) simplifica o acesso a inúmeros sites públicos e privados. A eID é gerada através de um sistema criptográfico assimétrico multifator, através de duas chaves, uma privada e outra pública: a primeira assina o documento, a segunda permite ao destinatário verificar a autenticidade da assinatura e a não alteração do conteúdo. A assinatura digital assimétrica garante um elevado grau de segurança jurídica de autenticidade quando ao seu autor e à integridade do documento (Correia, 2024; Pena, 2020; Silva, 2024).

O CC e a CMD permitem, ainda, a assinatura de documentos digitais através da AEQ, com as funções que desempenha, enquanto profissional, bastando associar os atributos ao

SCAP, estabelecendo os requisitos seguintes para acesso aos atributos profissionais (ARTE, 2025f) empresariais, dirigentes públicos, eleitos locais e funcionários (Silva, 2024). Ora, tendo em conta o objeto do presente trabalho, salientamos que apenas é possível associar os atributos profissionais de elementos da PSP na qualidade de dirigentes, cujas funções tenham sido publicadas em DRE (ARTE, 2025g) [(art.º 10.º Decreto-Lei n.º 83/2016, de 16 de dezembro e art.º 11.º da Portaria n.º 73/2018, de 12 de março)].

O Regulamento (EU) n.º 910/2014, de 23 de julho (eIDAS), estabeleceu um quadro comum da eID e autenticação, facilitando transações transfronteiriças, através de serviços de confiança, garantindo a interoperabilidade e reconhecimento mútuo entre Estados Membros (EM), viabilizando a autenticação segura, através dos sistemas de credenciação nacionais notificados à Comissão Europeia (CE). A CE disponibiliza uma plataforma (ARTE, 2025h) para autenticação do certificado digital atribuído pelo país de origem noutro EM. Mais recentemente, o regulamento (EU) 2024/1183, de 11 de abril introduziu no eIDAS a Carteira Digital Europeia (CDE), permitindo armazenar e utilizar documentos oficiais em todos os países da EU. A CDE permite comprovar a eID de cidadãos e empresas que acedam a serviços públicos e privados, conservando, gerindo dados da identidade e documentos em formato digital. A emissão CDE cabe a cada EM e será, legalmente, aceite nos restantes.

O Decreto-Lei n.º 12/2021, de 9 de fevereiro veio consolidar a validade, eficácia e valor provatório dos documentos eletrónicos, bem como o SCEE- PKI de acordo com o eIDAS.

Poderemos, assim, concluir, que o ecossistema tecnológico e legal nacional e europeu da eID promove a eficiência administrativa, a confiança e a segurança no ambiente digital, garantindo que os cidadãos da UE, conseguem autenticar-se e efetuar transações com a eID em qualquer EM de forma acessível, segura e protegida.

2.2.1. O Alicerce: A Identidade Eletrónica do Cidadão

No ano de 2006, foi lançado o Programa Simplex[3], iniciativa de inovação e modernização administrativa que almejava uma AP mais eficiente, transparente e próxima do cidadão (Cardoso, 2018; Carvalho, 2020). O Simplex destacou-se como pioneiro na reforma digital, antecipando programas de países europeus de referência como a Estónia (Magalhães et al., 2025).

[3] Programa criado em 2006 pelo Governo português, que visava modernizar processos, desmaterializar procedimentos e melhorar a eficiência e transparência da administração pública.

Este programa impulsionou a criação de estratégias públicas assentes em TIC, permitindo desenvolver serviços públicos mais rápidos e eficazes (Rito et al., 2019). Do esforço resultou o Governo Eletrónico (*e-Gov*), que, centrado no cidadão, promoveu serviços online e reduziu significativamente a procura presencial junto dos organismos públicos (Carvalho, 2020; Dias & Gomes, 2021; Rito et al., 2019; Viana, 2021).

A Lei n.º 7/2007, de 5 de fevereiro, instituiu o CC, instrumento científico/tecnológico que possibilita a identificação digital segura, dispondo de dados pessoais cifrados e dois certificados: autenticação, ativado no momento do levantamento; AEQ, de ativação facultativa (Barbosa, 2010; Pena, 2020; Rito et al., 2019). Posteriormente, a Lei n.º 19-A/2024, de 7 de fevereiro, atualizou tecnologicamente e fisicamente o CC, alinhando-o com as normas de harmonização europeias (ARTE, 2025i).

Já a Lei n.º 37/2014, de 26 de junho, criou a CMD, que simplificou o acesso a serviços digitais através de autenticação multifator: palavra-passe e código PIN enviado por SMS (*Short Message Service*) para o telemóvel associado ao CC. A CMD possibilita também a assinatura de documentos eletrónicos (Correia, 2024; Pena, 2020).

Figura 1

Certificado da CMD de acordo com o regulamento eIDAS


apcer

Certificado
Certificate

NÚMERO 2018/DTAE.0006

O Serviço Eletrónico de Confiança de Certificados Qualificados de Assinaturas Eletrónicas da

AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA, I.P.
Rua de Santa Marta, 55
1150-294 LISBOA
PORTUGAL

cumpre os requisitos do

Regulamento (UE) nº 910/2014

e

ETSI EN 319 401 V2.3.1, ETSI EN 319 411-1 V1.3.1, ETSI EN 319 411-2 V2.4.1, ETSI EN 319 412-2 V2.2.1,
ETSI EN 319 412-5 V2.3.1, Despacho 154/2017 do GNS, Despacho 155/2017 do GNS, Despacho 2705/2021 do GNS

IPAC

Emitido em 2024-04-15
Válido até 2026-04-29

José Leitão
CEO

Fonte: De "Assinatura Digital", de ARTE, 2024, https://www.autenticacao.gov.pt/web/guest/cmd-assinatura

O Instituto dos Registos e do Notariado (IRN) é responsável pela emissão, renovação e gestão do CC, incluindo a validação de identidades e a emissão de certificados eletrónicos, assim como pela proteção de dados. Já a Agência de Modernização Administrativa (AMA)

focalizou-se na simplificação administrativa, modernização digital e gestão do atendimento físico e eletrónico, promovendo a interoperabilidade da AP (AMA, 2022).

Com a entrada em vigor do Regulamento eIDAS, a AMA notificou a CE sobre os sistemas de identificação eletrónica em Portugal, nomeadamente a ADQ e a CMD (art. 7.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro e arts. 6.º e 9.º do eIDAS).

O Decreto-Lei n.º 96/2025, de 21 de agosto, substituiu a AMA pela Agência para a Reforma Tecnológica do Estado (ARTE). Esta nova entidade, liderada por um *Chief Technology Officer* (CTO), tem como intenção posicionar Portugal, até 2030, entre os dez países digitalmente mais avançados. A ARTE proporciona uma visão coordenada da infraestrutura tecnológica do Estado, garantindo a homogeneidade das políticas digitais, a coordenação centralizada e a interoperabilidade, em articulação com setor privado, academia e sociedade civil.

Por sua vez, o Decreto-Lei n.º 94/2024, de 28 de novembro, suprimiu o Centro de Gestão da Rede Informática do Governo (CEGER), incorporando alguns serviços na ARTE, particularmente a emissão de certificados digitais para titulares de altos cargos da AP. O SCAP permite associar atributos profissionais, empresariais e públicos (art. n.º 546.º do Código das Sociedades Comerciais) ao CC e à CMD, conferindo poderes legais para assinatura eletrónica de documentos, incluindo a qualidade profissional para a prática do ato. Por outro lado, o DRE tornou-se a plataforma oficial de publicação de atos jurídicos, com plena eficácia legal.

Relativamente ao SCEE (art.º 23.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro e art.º 25.º eIDAS), responsável pela PKI, confere a segurança das transações eletrónicas através de serviços de autenticação e assinatura digital e proporciona três princípios fundamentais: Autenticidade – confirmação da assinatura mediante correspondência entre chave pública e privada; Integridade – proteção contra alterações no conteúdo após a assinatura; Não repúdio – impossibilidade de negar a autoria da assinatura (Cardoso, 2012; Pena, 2020; Rito et al., 2019).

A evolução da identidade eletrónica em Portugal, desde o Simplex até à constituição da ARTE, evidencia um percurso de modernização contínua. A conjugação de legislação, entidades especializadas e sistemas tecnológicos robustos sedimentou a confiança digital e posicionou o cidadão no centro das políticas públicas. O desafio para 2030 será assegurar não só a interoperabilidade nacional e europeia, mas também a inclusão e competitividade do país na sociedade digital.

2.2.2. A Garantia Jurídica: O Regulamento eIDAS e a Assinatura Eletrónica Qualificada (AEQ)

O eIDAS, criou um quadro legal comunitário, visando o reconhecimento mútuo e a aceitação transfronteiriço da eID, garantindo autenticação segura de credenciais nacionais. A CE, disponibiliza uma plataforma (CE, 2025a), onde o cidadão se pode autenticar com o certificado digital noutro EM. Portanto, procura-se que cidadãos, empresas e autoridades públicas, obtenham confiança e segurança nas transações online, fundamentais para o desenvolvimento económico e social dos EM (Correia, 2024; Oliveira, 2024; Ruiu et al., 2024).

O regulamento introduziu outros meios de eID como: assinaturas eletrónicas; selos eletrónicos; selos temporais, entre outros, todos com eficácia legal e admissível como meio de prova, procurando aumentar a eficiência dos serviços eletrónicos públicos e privados nas transações eletrónicas, através do reconhecimento e aceitação mútua entre EM (Correia, 2024; Oliveira, 2024). O eIDAS instituiu normas para as entidades na produção de meios de eID, nomeadamente o nível de supervisão, responsabilidade, requisitos técnicos de segurança e obrigatoriedade de reconhecimento dos serviços dos prestadores por outro EM (Correia, 2024; Oliveira, 2024). O n.º 1 do art. 3.º do eIDAS define "«identificação eletrónica»: o processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva". Já o n.º 35, define "«documento eletrónico» como qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual". Por último, o art. 46º do eIDAS consagra que não podem ser recusados os efeitos legais, nem a admissibilidade, dos documentos eletrónicos em processo judicial, pelo simples facto de se encontrar em suporte eletrónico, estando, inequivocamente, reconhecido, no artigo 25º, que a AEQ tem efeito legal equivalente ao de uma assinatura manuscrita.

O Decreto-Lei n.º 12/2021, de 9 de fevereiro consolidou a legislação já existente relativa à validade, eficácia e valor provatório dos documentos eletrónicos e sobre o SCEE - PKI. A noção de documento do art. 362.º do Código Civil (C.C.) não faz referência a qualquer tecnologia específica, mantendo-se a norma válida, independentemente da evolução tecnológica. Poderemos, assim, considerar como documentos autênticos diferentes meios tecnológicos, sejam analógicos ou digitais. A conjugação do art. 363.º n.º 1 com o art. 368.º do C.C. permite uma interpretação extensiva, abrangendo todos os meios eletrónicos

atuais (e-mails, gravações digitais, mensagens, *WhatsApp*, entre outros). O legislador quis dar relevo probatório a "quaisquer outras reproduções de factos ou de coisas", e, assim reconhecer o valor provatório, como se de originais se tratasse.

O art. 3.º, n.º 5 do Decreto-Lei n.º 12/2021, de 9 de fevereiro indica que, quando seja aposta uma AEQ o documento eletrónico, cujo conteúdo seja suscetível de representação como declaração escrita, tem a força probatória de documento assinado (Rito, 2018), conforme art. 376.º do C.C. Por outro lado, o n.º 6 do citado decreto refere que quando é aposta uma AEQ e o documento eletrónico não seja suscetível de representação como declaração escrita tem a força probatória prevista no artigo 368.º do C.C. e no art. 167.º do CPP. A AEQ é uma assinatura eletrónica avançada que está de acordo com a legislação europeia e nacional, resultando de uma sucessão eletrónica de tratamento de dados, associando, inegavelmente, o assinante ao documento eletrónico e à integridade do documento, atribuindo-lhe o mesmo valor jurídico que uma assinatura manuscrita (Rito et al., 2019). Em 2024, Correia diz-nos que a assinatura digital de criptografia assimétrica, com chave pública, é o modelo de identificação eletrónica constante no eIDAS.

A assinatura eletrónica é gerada através de um sistema criptográfico assimétrico, que assenta na geração de um par de chaves, uma privada e outra pública. O titular, ao utilizar a chave privada, apõe a sua assinatura no documento eletrónico em concordância com o seu conteúdo, atestando a sua autoria. A chave pública permite ao destinatário do documento atestar que a assinatura resulta da utilização da chave privada, garantindo a sua autoria, e que o conteúdo não se alterou depois de aposta a assinatura. A confirmação de uma assinatura digital assimétrica garante um elevado grau de segurança jurídica de autenticidade quanto ao seu autor, à integridade do conteúdo do documento, comprovando que a assinatura foi aposta pelo seu titular e que o documento não sofreu alterações após o envio ao destinatário (Correia, 2024; Pena, 2020; Rito et al., 2019; Rito, 2018).

Ora, um documento assinado nestes termos possui o mesmo valor legal que uma assinatura manuscrita e assinado pelo seu autor (art. 3.º n.º 2 e art. 6.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro e art.º 25.º do eIDAS), sendo plenamente admissível em tribunal ou qualquer procedimento administrativo ou contratual (Tribunal da Relação Coimbra, 2017). Como refere o n.º 12 do art.º 3.º "«Assinatura eletrónica qualificada»: é uma assinatura eletrónica avançada, criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica". Para a assinatura eletrónica ter valor, é necessário o seu titular deter um certificado válido por uma entidade, que o eIDAS designa por "prestador de serviços de confiança", fazendo a

distinção entre os qualificados e não qualificados (n.º 19.º e 20.º do art. 3.º), prestador que segundo o art. 6.º e 28.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro, é credenciado pelo Gabinete Nacional de Segurança (GNS) [(n.º 3.º al. j do art. 2.º do Decreto-Lei n.º 3/2012, de 16 de janeiro)]. Assim, apenas o documento eletrónico que tenha aposta uma AEQ efetuada sob o respaldo de um certificado emitido por prestador credenciado pelo GNS possui força provatória (n.º 5 do art. 3.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro). Do mesmo modo, o n.º 6 do art.º 3.º atribui valor probatório aos documentos eletrónicos que não revistam forma escrita, desde que tenha aposta uma AEQ, cujo suporte encontramos nos art. 368º do C.C. e 167º do CPP. Assim, se nos dois casos referidos o prestador não se encontre legalmente credenciado, estaremos perante uma assinatura eletrónica avançada, pelo que o documento embora escrito e assinado, não tem força probatória plena, sendo apreciado segundo o livre arbítrio do julgador (n.º 10 do art. 3.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro).

2.2.3. A Lacuna Teórica e Prática: A Ausência da Identidade Profissional

A AEQ, utilizada através do CC ou da CMD, permite confirmar a identidade do cidadão. A eID produzida através de um desses mecanismos possui, por lei, igual valor jurídico à assinatura manuscrita, tanto em Portugal como nos restantes EM da UE (art. 3.º, n.ºs 2 e 6, e art. 6.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro e art. 25.º do Regulamento eIDAS). O documento eletrónico com a eID que não possa ser apresentado como declaração escrita tem a força probatória de documento assinado manualmente, não podendo ser recusado em processo judicial pelo fato de se apresentar em suporte eletrónico (art.º 25.º do eIDAS).

Não obstante, a AEQ apenas atesta a identidade do titular, não certificando atributos ou poderes profissionais. Em Portugal, essa função é assegurada pelo SCAP, que permite associar os atributos empresarias e públicos (administradores, gerentes, diretores e procuradores) ao CC e CMD, incluindo na AEQ os atributos e a entidade que validou (art. 12.º da Portaria n.º 73/2018, de 12 de março), reconhecendo a qualificação profissional e os poderes inerentes ao cargo desempenhado. Contudo, o artigo 11.º do SCAP limita a certificação de atributos públicos aos dirigentes cujas funções tenham sido publicadas em DRE (art. 10.º do Decreto-Lei n.º 83/2016, de 16 de dezembro). A AMA publica a lista de associações públicas profissionais aderentes ao SCAP (ARTE, 2025k), na qual consta a PSP,

mas em termos legais, apenas os diretores da PSP com funções publicadas em DRE podem requerer a certificação do atributo público (ARTE, 2025l).

Por outro lado, com a desmaterialização dos atos policiais em formato eletrónico, destinados à publicação no DRE, bem como da remessa dos autos de infração rodoviária para a Imprensa Nacional Casa da Moeda (INCM), a PSP procedeu à credenciação, através do CEGER de alguns Oficiais e Chefes afetos às Esquadras de Trânsito, com a finalidade de assinar os autos com o cartão do CEGER. Todavia, ainda que disponha, do ponto de vista técnico, da tecnologia necessária para a eID com os respetivos atributos, devido a requisitos de licenciamento ou credenciação o seu uso encontra-se restrito à assinatura de autos no Sistema de Contraordenações de Trânsito (SCOT).

De igual modo, em 2012, a Direção Nacional da PSP, credenciou, através do cartão emitido pelo CEGER, diversos Oficiais da PSP (Despacho n.º 29/GDN/2012), contendo a eID os atributos inerentes às funções de responsabilidade, publicadas no DRE.

Assim, constatamos que apenas têm acesso à AEQ com os atributos profissionais, uma percentagem restrita de dirigentes da PSP, nomeados em DRE, excluindo, assim, a vasta maioria dos polícias que praticam atos de polícia judiciária (APC e OPC) e de polícia administrativa. Atendendo ao acima exposto, os restantes elementos policiais, ao utilizarem o CC com a AEQ, sem os atributos profissionais, apenas atestam a qualidade de cidadão e não de OPC, podendo ser colocado em causa a legitimidade e a validade jurídica do ato processual, assinado com a AEQ sem conter os atributos profissionais (art. 55.º do CPP, art. 2.º, 3.º e 10.º da Lei da Organização da Investigação Criminal (LOIC) e art. 3.º al. e) da Lei n.º 53/2007, de 31 de agosto).

Dos planos estratégicos da PSP, com peculiar relevância para o presente estudo, salientamos a EPSP 23/25, que evidencia o PESI2 como o motor tecnológico da PSP, estratégia que, já em 2002, no eixo digital, previa a emissão de cartões eletrónicos digitais na PSP. Por outro lado, os objetivos estratégicos do MP, para o triénio 2025/2027 (MP, 2025), procuram integrar os sistemas de suporte da atividade processual dos diversos OPC, buscando eficiência processual através da desmaterialização digital. Nesse seguimento, foi concedida autorização à PSP para adquirir software de interoperabilidade de apoio à atividade dos tribunais e do sistema estratégico de informação da PSP (Portaria 762/2024, de 28 de outubro).

Obviamente que, se o MP procura a desmaterialização processual com os OPC e a PSP vai adquirir software de interoperabilidade necessário para a desmaterialização entre os dois organismos, será uma medida fundamental desenvolver uma solução que permita aos

polícias terem uma identidade profissional com os atributos profissionais, o que passará, indubitavelmente pela evolução tecnológica do bilhete de identidade policial, agora existente, medida fundamental e primordial na transformação digital da PSP.

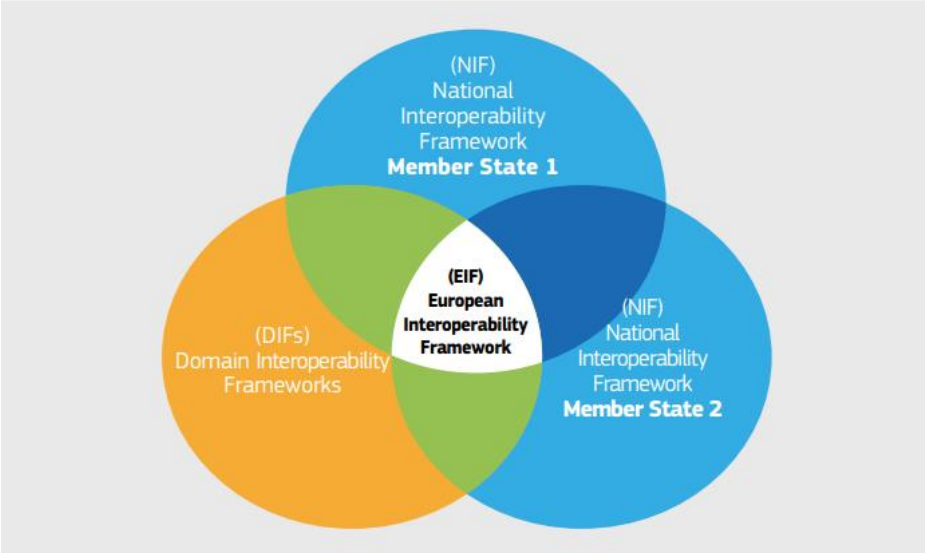
2.3. Interoperabilidade e os Desafios Sociotécnicos na Cultura Policial

A Resolução do Conselho de Ministros n.º 42/2015, de 19 de junho evidencia a prioridade no desenvolvimento da iAP, salientando a importância do *e-Gov*, como fator impulsionador da competitividade da economia, apresentando-se como a pedra basilar na partilha entre sistemas e entre entidades (Parisopoulos, et al., 2007). As estratégias de Portugal e UE, para a interoperabilidade, preservação digital e dados abertos, resulta do Regulamento Nacional de Interoperabilidade Digital e do Regulamento eIDAS, evidenciando-se o balcão único para soluções e cooperação comunitária.

Embora cada Estado-Membro da União Europeia detenha o seu próprio quadro jurídico nacional, a norma da interoperabilidade europeia assegura que organizações sujeitas a diferentes sistemas jurídicos, políticas ou estratégias possam cooperar de forma eficaz. Para isso, impõe a celebração de acordos claros, prevenindo bloqueios e assegurando que os serviços públicos europeus digitais sejam interoperáveis na UE e entre os EM (Almeida, 2019).

Figura 2

Estrutura europeia de interoperabilidade



Fonte: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

A interoperabilidade é um dos maiores desafios da PSP, pois a colaboração entre instituições não se basta na simples interoperabilidade de informação, incluindo, também a dimensão tecnológica, assente em equipamentos de comunicação (Felgueira et al., 2019). Para Morgado et al. (2024) o desenvolvimento das TIC é a força motriz da mudança policial, com grande enfoque na interoperabilidade, sendo a tecnologia fundamental no apoio à decisão e no cumprimento da função policial; no entanto, a tecnologia para usuários encontra-se obsoleta, pela ausência de rapidez e de acesso a tecnologias avançadas. Os sistemas tecnológicos da PSP, como bases de dados, softwares e plataformas distintas patenteiam a carência de coordenação e interoperabilidade entre sistemas (Felgueiras et al., 2019).

Para melhor compreensão, abordaremos, resumidamente, os diferentes níveis de interoperabilidade: técnica (ARTE, 2025m) - permite que dois ou mais repositórios/plataformas/aplicações de software troquem dados entre si, de forma segura, sem qualquer custo, atingindo um objetivo comum (Sacramento et al., 2015); organizacional (ARTE, 2025n) - capacidade das organizações, através de modelos de arquitetura trabalham em rede, cooperam entre si, definem papéis e responsabilidades, evitando o desperdício de recursos (Fialho, 2022); semântica (ARTE, 2025o) - processamento e interpretação correta da informação entre os diversos sistemas, garantindo a interpretação evidente por parte do recetor "o que é enviado é o que é compreendido", assegurando, ainda, a forma da estrutura linguística utlizada (Fialho, 2022); legal (ARTE, 2025p) – a qual considera as normas legais individuais e coletivas na livre circulação de dados (Leese, 2024).

A PSP é uma organização com características diferenciadas, os seus polícias são confrontados pelo risco constante, dependente do uso da “força” uma forte identificação com a farda, em prol da segurança pública (Viriato, 2023). A tradição da organização e a hierarquia vertical têm de conciliar o desafio da manutenção da disciplina e da ordem com a inevitável abertura à inovação e mudança (Freitas & Barth, 2011). Apesar da introdução progressiva de novas tecnologias, é essencial, que os profissionais, reconheçam as suas vantagens e o impacto positivo que podem ter no desempenho. Só assim será possível ultrapassar barreiras de natureza cultural, em particular a falta de competências digitais e a resistência institucional à mudança (Matte et al, 2021; Riskasari & Ibrahim, 2025). A evolução para um cartão policial digital poderá trazer tensões internas, marcadas pela

resistência à mudança, gerando dificuldades na sua implementação (Duarte, 2005; Gonçalves & Neves, 2012), mas, por outro lado, proporciona eID forte com atributos profissionais, garantindo segurança jurídica, além de autenticidade, integridade e não repúdio e, como medida racional e de elevado retorno, permite uma desmaterialização dos processos criminais, que são a grande percentagem do expediente produzido na PSP, sem deixar de dar relevância aos PA.

2.4. O Acto Policial Digital: Implicações, Validade e a Fronteira da Prova

A segurança da eID é suportada por procedimentos e certificados qualificados, que atesta os dados pessoais e a sua integridade, contribuindo para a segurança e confiança dos usuários, cuja validade jurídica é assegurada pelas entidades fornecedoras do certificado, sendo essa validade reconhecida quer em legislação nacional e europeia sobre eID (Morgado & Mendes, 2016). Não obstante, os policias utilizarem eID, sem conter os atributos profissionais, consideramos que a assinatura será na qualidade de um simples cidadão e não de OPC, podendo esse documento ser juridicamente colocado em causa, pois poderá não garantir a legitimidade processual e a qualidade de OPC.

Para Morgado e Mendes (2016), "a segurança jurídica serve por um lado para estabilizar as relações jurídicas – âmbito objetivo – e, por outro, proteção de confiança – âmbito subjetivo" (p. 13). Esta segurança jurídica encontra-se regulada num conjunto de normas jurídicas que regulam a prova digital (Lei n.º 32/2008, de 17 de julho, Lei n.º 109/2009, de 15 de setembro, Decreto-Lei n.º 12/2021, de 9 de fevereiro e o eIDAS), concorrendo para aumentar os níveis de confiança e segurança, procurando reduzir os riscos dos direitos fundamentais. Ainda assim, a prova digital é, muitas vezes, contestada, obrigando ao uso de instrumentos digitais para atestar a autoria e receção. A mesma será legal e reconhecida como prova, se existir uma prova digital válida e a autoria não for contestada; no entanto, mantêm-se o princípio da livre apreciação da prova do julgador (art. 127.º CPP). Por outro lado, a prova digital é instável e facilmente alterável, sendo versátil, podendo comprometer a conservação da prova; além disso, é mais lesiva dos direitos fundamentais do que os meios de obtenção de prova tradicionais, discretos, encobertos, e empregam tecnologia disruptiva, fora do alcance do homem médio (Lambelho, 2022; Siscari, 2025). O âmbito probatório encontra-se delimitado pela Constituição; por conseguinte, a utilização de meios de prova obtidos em desconformidade com as normas

legais atenta contra a dignidade da pessoa humana, pondo em causa a legitimidade do Estado e o exercício do seu poder sancionatório. (Costa, 2017).

3. Método

O presente estudo considera-se ser uma mais-valia, porque a pesquisa bibliográfica realizada não identificou estudos prévios focados na implementação de um cartão policial digital na PSP, indicando uma lacuna na literatura e, justifica a presente investigação. Assim a nível metodológico, estamos perante um Estudo Teórico (Quivy & Campenhoudt, 2005), de natureza exploratória e de finalidade aplicada (Júnior et al., 2022). O presente trabalho enquadra-se numa investigação qualitativa, baseada na análise documental profunda, alicerçando-se o seu corpus em: legislação, dissertações, relatórios técnicos, obras literárias, documentos da união europeia, IA act, artigos e trabalhos científicos (Bravo, 1988), sustentado em trabalhos de diferentes autores que estudam esta temática, conscientes que, tal como refere Quivy e Campenhoudt (2005) "as leituras ajudam a fazer o balanço dos conhecimentos relativos ao problema de partida" (p. 69).

O problema de investigação foi o resultado profundo da revisão de literatura, cumulativamente com a experiência adquirida pelo autor, no âmbito do desempenho de funções de liderança no sistema de Investigação Criminal da PSP. Nos últimos anos, foram identificados alguns constrangimentos práticos dentro da PSP, que não permitiram à instituição acompanhar as transformações tecnológicas de outras organizações públicas (PESI2), pelo que, a crescente digitalização de processos e o fato de todos os elementos da PSP não possuírem uma AEQ contendo os atributos profissionais, leva a que não exista uma otimização e automação de processos e consequentemente aumento da eficiência organizacional.

Baseados na pergunta de partida já invocada e segundo a abordagem de Quivy e Campenhoudt (2005), apresentam-se as seguintes perguntas derivadas (PD): i) Como garantir que os elementos policiais têm associados os atributos profissionais na assinatura eletrónica? ii) Será pertinente a evolução para um cartão policial digital, tendo em vista a contínua redução do expediente físico? iii) Quais os riscos de contestação jurídica dos atos, caso não tenham associados à assinatura eletrónica os atributos profissionais?

4. Perspetivas

A EPSP25/27 aposta na inovação, desenvolvimento e modernização como fator crítico de sucesso, salientando que o motor tecnológico da PSP é o PESI2. Apesar de, no plano estratégico PESI2, se encontrar previsto a emissão do cartão policial digital, esse avanço tecnológico não sucedeu: em primeiro lugar por mero impedimento legislativo na atribuição do atributos profissionais na AEQ; em segundo lugar por falta de investimento, potenciado também, pela grande maioria dos dirigentes terem acesso à AEQ com o CC ou com o cartão do CEGER com os atributos profissionais, permitindo a assinatura de atos que estão delegados ou subdelegados nesses oficiais. O cartão policial digital na PSP, permitirá acelerar a modernização administrativa e a transformação tecnológica digital na instituição, ao mesmo tempo, favorecer a simplificação de PA e, consequentemente a melhoria da eficiência, redução de custos e recursos humanos. Permitirá, ainda, aos polícias deter uma eID com os atributos profissionais, isto é, com indicação formal da sua qualidade de OPC, garantindo a validade legal dos documentos eletrónicos em atos processuais delegados pelo MP. Admite a utilização, como método alternativo, ao modelo de autenticação atual, que revela fragilidades de segurança, obrigando os usuários a memorizar diversas credenciais, atendendo às diversas aplicações existentes na PSP. A assinatura digital assimétrica garante um elevado grau de segurança jurídica de autenticidade quanto ao seu autor e à integridade do documento, sendo válida para efeitos judiciais; no entanto, no presente estudo, ficou claro que os polícias, ao assinarem um documento eletrónico, necessitam de ter os atributos profissionais associados; se não fosse assim, porque precisariam os dirigentes dos atributos no CC e no cartão CEGER?

Se um documento eletrónico for assinado com a AEQ, mas sem a incorporação dos atributos profissionais do agente policial, entende-se que tal ato pode carecer de validade jurídica, uma vez que a assinatura não incorpora os poderes necessários para a prática do ato. Admite-se, no entanto, que esta condicionante poderia ser mitigada caso o documento, ao ser assinado com a AEQ do CC, inclua no seu corpo a identificação expressa do agente, incluindo nome e posto. Todavia, importa salientar que a plataforma Sistema Estratégico de Informação (SEI) não permite que, junto ao local da assinatura, sejam automaticamente acrescentados esses elementos de identificação funcional.

Deste modo, subsiste um risco de insegurança jurídica, uma vez que a omissão de atributos profissionais associados à assinatura eletrónica pode gerar dúvidas na tramitação digital dos processos judiciais entre a PSP e o MP. Tal cenário é indesejável e pode

comprometer a credibilidade institucional, pelo que se requer a adoção de alternativas que certifiquem a plena validade e legitimidade dos atos praticados digitalmente pelos elementos policiais.

É provável que esta evolução tecnológica do cartão digital policial tenha de ser implementada por força da Portaria n.º 280/2013, de 26 de agosto, que aponta a tramitação eletrónica dos processos como obrigatória na fase de inquérito dirigida pelo MP. Ora os OPC são quem coadjuvam os titulares dos inquéritos na fase do inquérito[4], conforme previsto no art. 270.º do CPP.

No tocante a este assunto, o modelo de Cartão de Identificação (CI) do pessoal da PSP, regulado pela Portaria n.º 441/2006, de 9 de maio, destina-se exclusivamente à identificação dos elementos da PSP no ativo, em situação de pré-aposentação fora da efetividade de serviço e na aposentação. Nos termos dos artigos 18.º e 20.º do Estatuto Profissional da PSP, o CI constitui o meio oficial de identificação profissional dos polícias.

Atualmente, o cartão integra apenas um código de barras destinado à identificação dos beneficiários familiares do subsistema de saúde da PSP (SAD/PSP), não dispondo de qualquer componente tecnológica avançada, como chips de autenticação ou sistemas digitais de verificação.

No âmbito do presente estudo, verificou-se que outros países europeus, designadamente França e Espanha, já desenvolveram e implementaram modelos de cartão digital em conformidade com as normas eDIAS. Esta modernização permite uma identificação mais segura e multifuncional, em contraste com o modelo português ainda assente em tecnologia tradicional.

Figura 3

Cartão de Identificação da PSP

[4] Delegação genérica de competências na PSP

Fonte: https://files.diariodarepublica.pt/1s/2006/05/089b00/32653269.pdf

Figura 4

Documento de identificação do Cuerpo Nacional de Policía.

Fonte: https://www.boe.es/buscar/pdf/2007/BOE-A-2007-6604-consolidado.pdf

Figura 5

Cartão de identificação profissional Gendarmerie Nationale

Fonte: https://www.pandore-gendarmerie.org/renouvellement-des-cartes-professionnelles-electroniques/

Tabela 1

Quadro comparativo do Cartão de Identificação da PSP, Gendarmerie e Cuerpo Nacional de Policía

País/Instituição Policial	Tipo de cartão e funcionalidades
Portugal - PSP Portaria 441/2006, de 9 de maio	- Bilhete de identidade em PVC; - Não integra qualquer solução digital para a identificação eletrónica; - Permite a identificação visual; - Código de barras permite identificação de beneficiário SAD/PSP.
França - Gendarmerie Nationale[5]	- Cartão eletrónico digital; - Contém duplo chip: contacto e sem contacto/NFC; - Permite autenticação, confidencialidade e assinatura; - Identificação profissional; controlo de acessos; - Certificado da assinatura conforme requisitos eIDAS; - Ao titular do certificado é entregue a chave privada.
Espanha - Cuerpo Nacional de Policía[6]	- Cartão eletrónico Digital; - O chip contendo os certificados eletrónicos;

[5] https://insigniaspoliciales.com/en/other-countries-id-cards/5715-gendarmerie-nationale-id-card.html
[6] https://www.boe.es/buscar/pdf/2007/BOE-A-2007-6604-consolidado.pdf

	- Identificação eletrónica, para assinar documentos e encriptar dados; - Emissão de outros cartões (alunos em formação e outros funcionários; - Certificados válidos por 4 anos; - Cartão entregue presencialmente com código secreto para - ativar o cartão; - Emissão de novo cartão, case mude de funções ou de categoria.

Fonte: Elaborado pelo próprio

5. Conclusão e discussão

As políticas estratégicas de Portugal e da UE tem como foco o desenvolvimento de uma cultura de segurança digital centrada nas pessoas e nas empresas, apostando no desenvolvimento das competências digitais de cidadãos, empresas e AP. A transformação digital e a modernização administrativa em Portugal estão alinhadas com a UE, havendo áreas em que o país é considerado líder digital (CE, 2025b), como foi o caso recente da identidade digital europeia eIDAS.

A incorporação de ferramentas tecnológicas pela PSP, tem vindo a alterar significativamente as práticas tradicionais, demonstrando que o futuro da atividade policial passa inevitavelmente pela inovação digital, quer para garantir um modelo de policiamento tecnológico, quer para responder eficazmente às exigências da sociedade contemporânea, acompanhando a evolução digital da AP em Portugal e na UE. (Azevedo, 2023; Guimarães, et al., 2025). São necessários líderes digitais que promovam e desenvolvam estratégias no mundo digital, transversais a toda organização, estimulando uma cultura de inovação digital, garantindo que o público interno acompanha esse salto tecnológico (Ravesteyn & Ongena, 2019).

Nessa perspetiva, ao potenciar os serviços digitais através, do cartão digital, a PSP busca o equilíbrio entre dois valores, estando de um lado, a eficiência, otimização e redução de custos e, por outro, a autenticação, legitimidade e segurança dos documentos eletrónicos.

O cartão digital com os atributos profissionais seria uma mais-valia, promovendo a redefinição de autoridade policial nos atos processuais e administrativos, uma vez que o

elemento policial, ao praticar o ato, realiza-o na qualidade de OPC e não de cidadão, sendo claro que o ato seria praticado por quem tem autoridade e legitimidade. Por outro lado, o cartão polícia digital alavanca a digitalização em massa de processos na PSP, assumindo-se como referência de inovação digital entre as forças de segurança.

Contudo, há algumas debilidades que importa reconhecer. A resistência à evolução tecnológica, entre os polícias com menos literacia digital, pode contribuir para que alguns se sintam excluídos. Por outro lado, verifica-se uma acentuada relação de dependência dos sistemas informáticos, que, como sabemos, não estão isentos de falhas e, por isso, em situação de disrupção dos sistemas, requerem a existência de planos de contingência atuais, para manter operacional, tanto o back office como o front office. Para além disso, a transição digital pressupõe a realização de investimentos em infraestruturas e formação, o que pode representar uma limitação de natureza financeira e organizacional para a polícia.

De acordo com a análise formulada neste trabalho, foi plausível responder às perguntas derivadas inicialmente colocadas, atendendo ao enquadramento europeu e nacional. Podemos concluir que, em relação à PD i) na atualidade, a única forma dos elementos da PSP disporem de uma eID, com atributos profissionais adequados, será através da evolução tecnológica do cartão policial. No tocante à PD ii), a evolução do cartão policial configura uma inovação tecnológica que potencia a sustentabilidade e modernização da PSP. Esta solução tornará possível processos mais eficientes, redução de custos e uma gestão organizacional mais eficaz. Em relação à PD iii), a assinatura realizada com o CC, não comtemplando na eID o atributo profissional, pode não assegurar a legitimidade jurídica e a respetiva validade processual dos atos levados a cabo pelos polícias. Por conseguinte, entende-se que a resposta à pergunta de partida é positiva.

Não obstante as limitações temporais para a elaboração do presente estudo, acreditamos que o mesmo evidenciou um potencial extensivo a futuros investimentos e investigações que possam contribuir para a análise do impacto que o cartão digital terá na PSP.

Nessa perspetiva, apresentamos no Anexo 1 uma proposta detalhada de implementação do cartão profissional digital, que garante a eID com os atributos profissionais ao mesmo tempo que permite a autenticação, controlo de entradas e acesso a zonas de segurança. No âmbito da gestão dos atributos do cartão digital, importa que sejam garantidos através da integração do sistema de Gestão Integrada de Recursos da PSP (GIRe-PSP).

Este modelo de cartão policial, garante não só a uniformização da identidade digital dos polícias, mas também o alinhamento com a EPSP 23/25, o PESI2 e a ETDAP.

Por último, importa destacar que o suporte a padrões europeus e o cumprimento das normas eIDAS asseguram a interoperabilidade com sistemas de outros EM, reforçando a confiança dos cidadãos e promovendo a mobilidade e cooperação transnacional entre forças de segurança.

Referências bibliográficas

Almeida A. P. (2019). *O Papel da Interoperabilidade na Administração Pública: Contributos para melhorar a gestão de informação e a satisfação dos cidadãos.* Dissertação para obtenção de grau de Mestre em Administração Pública – MPA. Universidade de Lisboa. https://repositorio.ulisboa.pt/bitstream/10400.5/20412/1/1_Disserta%c3%a7%c3%a3o_Final.pdf

Almeida, P., & Ferreira, V. A. (2019). *Uma estratégia de modernização para a administração pública em Portugal.* In XXIV Congreso Internacional del CLAD sobre la Reforma del Estado y la Administración Pública (pp. 1-9).

AMA (2015, junho). Plataforma de Integração da Administração Pública (iAP-PI). https://www.iap.gov.pt/web/iap/plataforma-de-integracao

AMA (2022, s.d.). Relatório de atividades 2022. https://www.arte.gov.pt/web/arte/relatorios-de-atividades?p_p_auth=FXvoccMI&p_p_id=49&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&_49_struts_action=%2Fmy_sites%2Fview&_49_groupId=24077&_49_privateLayout=false

ARTE (2025a, setembro). Certificados digitais do Cartão de Cidadão. https://www.autenticacao.gov.pt/web/guest/certificados-digitais-do-cart%C3%A3o-de-cidad%C3%A3o

ARTE (2025b, setembro). Autenticação com Cartão de Cidadão. https://www.autenticacao.gov.pt/web/guest/cartao-cidadao/autenticacao

ARTE (2025c, setembro). Certificados Digitais do Cartão de cidadão. https://www.autenticacao.gov.pt/web/guest/certificados-digitais-do-cartão-de-cidadão

ARTE (2025d, setembro). Autenticação com Chave Móvel Digital. https://www.autenticacao.gov.pt/web/guest/chave-movel-digital/autenticacao

ARTE (2025e, setembro). Assinatura Digital com Chave Móvel Digital. https://www.autenticacao.gov.pt/web/guest/cmd-assinatura

ARTE (2025f, setembro). Sistema de Certificação de Atributos Profissionais. https://www.autenticacao.gov.pt/web/guest/a-autenticacao-de-profissionais

ARTE (2025g, setembro). Atributos de dirigentes públicos. *https://www.autenticacao.gov.pt/web/guest/atributos-profissionais/dirigentes-publicos*

ARTE (2025h, setembro). Autenticação Europeia. https://www.autenticacao.gov.pt/outros-meios/autenticacao-europeia

ARTE (2025i, setembro). O Cartão de Cidadão foi atualizado em 2024. https://irn.justica.gov.pt/Documentos-de-Identificacao/Cartao-de-Cidadao

ARTE (2025j, outubro). Plataforma de interoperabilidade, eIDAS. https://www.eid.as/

ARTE (2025k, setembro). Lista de entidades aderentes**.** https://www.autenticacao.gov.pt/entidades-aderentes

ARTE (2025l, outubro). Atributos de dirigentes públicos**.** https://www.autenticacao.gov.pt/web/guest/atributos-profissionais/dirigentes-publicos

ARTE (2025m, setembro). Interoperabilidade. Área Técnica. https://mosaico.gov.pt/areas-tecnicas/interoperabilidade

ARTE (2025n, setembro). Modelo de Interoperabilidade. Interoperabilidade organizacional. https://mosaico.gov.pt/areas-tecnicas/interoperabilidade/modelos/organizacional

ARTE (2025o, setembro). Modelo de Interoperabilidade. Interoperabilidade semântica. https://mosaico.gov.pt/areas-tecnicas/interoperabilidade/modelos/semantica

ARTE (2025p, setembro). Modelo de interoperabilidade. Interoperabilidade legal. https://mosaico.gov.pt/areas-tecnicas/interoperabilidade/modelos/legal

Azevedo, M. T. (2023). *Utilização de tecnologias móveis e o respetivo potencial operacional: Perceção dos Polícias das Esquadra Territoriais da Divisão Policial de Cascais do COMETLIS.* http://hdl.handle.net/10400.26/45768

Barbosa, A. M. (2010). *Cenários de utilização do cartão de cidadão em sistemas de informação académicos.* Faculdade de Engenharia da Faculdade do Porto.

Canelas, I. da C. de F. N. (2017). *Sistema estratégico de informação: O módulo de pedidos externos–dimensões da funcionalidade.* http://hdl.handle.net/10400.26/35136

Cardoso, J. (2012). *Da reforma administrativa ao e-government: 1974-2012 e-services no município de Pombal.* Dissertação de Mestrado em Ciências da Documentação e Informação, Faculdade de Letras. Universidade de Lisboa.

Cardoso, M. R. (2018). *Estratégias de Modernização Administrativa e Transformação Digital: Interoperabilidade e Integração no Sector da Agricultura e Floresta.* Instituto Universitário de Lisboa. https://repositorio.iscte-iul.pt/bitstream/10071/18661/4/master_maria_carneiro_cardoso.pdf

Carneiro, E. S. (2019). *Criação de valor público na era do governo digital: um ecossistema digital colaborativo.* Universidade Católica de Brasília.

Carmo, J. S. do, Rodrigues, M. A. de S., & Silva, B. C. (2025). Governança Digital e Modernização da Polícia Judiciária: Implementação de Procedimentos Policiais Eletrônicos como Ferramentas de Eficiência e Otimização de Recursos. *Temas Emergentes Da Nova Administração Pública Brasileira*, 8–30. https://doi.org/10.37885/241218501

Carvalho I. F. (2020). *A Modernização na Administração Pública: o caso do Programa Simplex.* Relatório de Estágio apresentado à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Administração Público-Privada. https://hdl.handle.net/10316/92668

Circular nº 6/2002, de 2002-03-11 do Procurador-Geral da República. https://www.ministeriopublico.pt/pagina/circulares

Comissão Europeia (2021, maio). Programa Europa Digital – um novo impulso para a digitalização das empresas. Comissão Europeia. https://digital-strategy.ec.europa.eu/pt/activities/digital-programme

Comissão Europeia (2024, julho). Construir o futuro digital. Comissão Europeia. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_pt#uma-abordagem-assente-em-tr%C3%AAs-pilares

Comissão Europeia (2025a, setembro). Autenticação Europeia. https://www.autenticacao.gov.pt/outros-meios/autenticacao-europeia

Comissão Europeia (2025b, junho). *Década Digital 2025*: Relatórios por país. https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports

Correia, M: J. A. (2024) - *Documentos electrónicos: um quarto de século - Lusíada.* Direito, (32) 183-200. http://hdl.handle.net/11067/7757

Costa, C. R. S. (2017). *As proibições de prova e a prova digital: Aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade* (Master's thesis), Universidade do Minho.

Decreto de 10 de abril de 1976, atualizado até à Lei n.º 1/2005, de 12 de agosto: Aprova a Constituição da República Portuguesa. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=4&tabela=leis

Decreto-Lei n.º 12/2021, de 9 de fevereiro, atualizado até ao Decreto-Lei n.º 94/2024, de 28 de novembro: Assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2021-156957575

Decreto-Lei n.º 243/2015, de 19 de outubro, atualizado até ao Decreto-Lei n.º 50-A/2024, de 23 de agosto: Aprova o estatuto profissional do pessoal com funções policiais da Polícia de Segurança Pública. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2015-114584637

Decreto-Lei n.º 262/86, de 2 de setembro, atualizado até ao Decreto-Lei 114-D/2023, de 5 de dezembro: Aprova o Código das Sociedades Comerciais. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1986-34443975

Decreto-Lei n.º 3/2012, de 16 de janeiro, atualizado até ao Decreto-Lei n.º 139-A/2023, de 29 de dezembro: Aprova a Lei Orgânica do Gabinete Nacional de Segurança. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2012-114157278

Decreto-Lei n.º 47 344, de 25 de novembro, atualizado até à Lei n.º 39/2025, de 1 de janeiro: Aprova o Código Civil e regula a sua aplicação. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1966-34509075

Decreto-Lei n.º 78/87, de 17 de fevereiro, atualizado até à Lei n.º 52/2023, de 28 de agosto: Aprova o Código de Processo Penal. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075

Decreto-Lei n.º 83/2016, de 16 de dezembro. Aprova o serviço público de acesso universal e gratuito ao Diário da República. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2016-122826417

Decreto-Lei n.º 94/2024, de 28 de novembro, atualizado até ao Decreto-Lei n.º 54/2025, de 28 de março: Procede à extinção, por fusão, do Centro de Gestão da Rede Informática

do Governo. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2024-898203717

Decreto-lei n.º 96/2025, de 21 de agosto: Reestrutura a Agência para a Reforma Tecnológica do Estado, IP (antiga Agência para a Modernização Administrativa, IP). https://diariodarepublica.pt/dr/detalhe/decreto-lei/96-2025-932837040

Decreto Lei n.º 243/2015, de 19 de outubro, atualizado até ao Decreto-Lei n.º 50-A/2024, de 23 de agosto: Estatuto Profissional do Pessoal com Funções Policiais da Polícia de Segurança Pública. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2015-114584637

Despacho Normativo n.º 38/2006, de 3 de agosto de 2006: Desmaterializa os processos de envio de actos para publicação nas 1.ª e 2.ª séries do Diário da República e fixa as regras de organização e publicação de actos na 2.ª série. https://diariodarepublica.pt/dr/detalhe/despacho-normativo/38-2006-31351344

Despacho n.º 29/GDN/2012, de 27 de dezembro da Polícia de Segurança Pública.

Dias, R., & Gomes, M. (2021). *Do governo eletrónico à governança digital: Modelos e estratégias de governo transformacional.* Ciências e Políticas Públicas/Public Sciences & Policies, 7(1), 93–117. https://doi.org/10.33167/2184-0644.cpp2021.vviin1/pp.93-117

Duarte, V. M. S. (2005). *Traços e perfis de cultura: estudo da cultura organizacional da Polícia de Segurança Pública de Braga.* Dissertação de Mestrado, Universidade do Minho.

Emery Y. e Giauque D. (2014). *The hybrid universe of public administration in the 21 st Century.* International Review of Administrative Sciences, Vol. 80(1) 23–32. https://doi.org/10.1177/0020852313513378

Estratégia Digital Nacional, (2025). Onde o Digital Simplifica. https://bo.digital.gov.pt/api/assets/etic/c508799d-8731-4a1f-b828-daac504c87e1/

Felgueiras, S., Pais, L. G., & Morgado, S. M. A. (2019). *Interoperability: Diagnosing a novel assessement model. European Law Enforcement Research Bulletin, Special Conference Edition: Innovations in law enforcement: Implications for practice, education and civil society,* (4), 255-260. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/339/301

Fialho, Y. R. (2022). *Interoperabilidade organizacional: uma abordagem com ontologia de processos intensivos em conhecimento e sistemas multiagentes.* Universidade de Brasília (UnB), no Programa de Pós-Graduação em Computação Aplicada.

Fortin, M. (2009). *O processo de investigação: Da conceção à realização.* (5ª ed.). (N. Salgueiro, Trad.). Lusociência – Edições Técnicas e Científicas.

Freitas, E. C. de, & Barth, M. (2011). Profissionalização da gestão nas empresas familiares: estagnar ou inovar? *Revista Brasileira De Gestão E Desenvolvimento Regional, 7*(3). https://www.rbgdr.net/revista/index.php/rbgdr/article/view/514

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: *finding the crossroads. Public management review*, 20(5), 633-646. https://doi.org/10.1080/14719037.2017.1327181

Gonçalves, S. P., & Neves, J. (2012). Caracterização da cultura organizacional em organizações policiais de Portugal. *Diaphora/Revista da Sociedade de Psicologia do Rio Grande do Sul* 12(2), Ago/Dez, pp. 01-13.

Governo de Português (2024, dezembro). *Estratégia Digital Nacional — Onde o digital simplifica*. Governo português. https://digital.gov.pt/estrategias/estrategia-digital-nacional

Guimarães, F., Moita, P., & Morgado, S. M. A. (2025). Enhancing law enforcement efficiency: A comparative study of manual and biometrics systems. *Hungarian Law Enforcement*, 25(Special Issue), 111-125. https://doi.org/ 10.32577/MR.2025.KSZ.1.7

Iacovino, N. M., Barsanti, S., & Cinquini, L. (2017). Public organizations between old public administration, new public management and public governance: the case of the Tuscany region. *Public Organization Review*, 17(1), 61-82.

Júnior A., Fernandes R. & Machado P., (2022), *Ciências Policiais. Conceito, Objeto e Método de Investigação Científica*. Instituto Superior de Ciências Policiais e Segurança Interna.

Lambelo, A. (2022). Algumas considerações sobre a utilização da prova digital em Direito do Trabalho. *Revista Jurídica Portucalense*, 22-37. https://doi.org/10.34625/issn.2183-2705(ne2v2)2022.ic-02

Leese, M. (2024). *AI and interoperability. In Handbook on Public Policy and Artificial Intelligence* (pp. 146-157). Edward Elgar Publishing.

Lei n.º 109/2009, de 15 de setembro: Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa (2009). https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174

Lei n.º 19-A/2024, de 7 de fevereiro, atualizada até ao Decreto-Lei n.º 20-A/2024, de 12 de fevereiro: Alteração às Leis n.os 7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização, 37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital, e 13/99, de 22 de março, que estabelece o novo regime jurídico do recenseamento eleitoral, e ao Decreto-Lei n.º 135/99, de 22 de abril, que define os princípios gerais de ação a que devem obedecer os serviços e organismos da Administração Pública na sua atuação face ao cidadão. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2024-840716423

Lei n.º 24-C/2022, de 30 de dezembro: Lei das Grandes Opções para 2022-2026. https://diariodarepublica.pt/dr/detalhe/lei/24-c-2022-205557191

Lei n.º 32/2008, de 17 de julho, atualizada até à lei n.º 18/2024, de 5 de fevereiro: Conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações electrónicas. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-174870511

Lei n.º 37/2014, de 26 de junho: Estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital. https://diariodarepublica.pt/dr/detalhe/lei/37-2014-25345579

Lei n.º 41/2013, de 26 de junho, atualizada até ao Decreto-Lei n.º 87/2024, de 7 de novembro Aprova o Código de Processo Civil. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2013-34580575

Lei n.º 49/2008, de 27 de agosto, atualizada até à Lei n.º 49/2008, de 27 de agosto: Aprova a Lei de Organização da Investigação Criminal. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-67191210-67192945

Lei n.º 53/2007, de 31 de agosto, atualizada até à Lei n.º 55-C/2025, de 27 de julho: Aprova a Lei Orgânica da PSP. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-174279072-174332731

Lei n.º 7/2007, de 5 de fevereiro, atualizada até à Lei n.º 19-A/2024, de 7 de fevereiro: Cria o cartão de cidadão e rege a sua emissão e utilização. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-70003493

Magalhães, F., Esteves, P., Gomes, A., & Almeida, A. P. (2025). *Trabalho GE 2024-2025 - O Simplex e a Transformação Digital da Administração Pública*. Faculdade de Direito da Universidade de Coimbra.

Matte, J., Welchen, V., da Costa, L. F., Fachinelli, A. C., Miri, D. H., Chais, C., & Olea, P. M. (2021). Evolução e tendências das teorias de adoção e aceitação de novas tecnologias. Editora Curitiva, *Revista Tecnologia e Sociedade*, 17(49), 102-117.

Ministério Público (2025). *Objetivos Estratégicos Triénio 2025-2027.* https://www.ministeriopublico.pt/sites/default/files/editor-files/objetivos-pgr-e-departamentos_15.1.24-alterado.pdf

Morgado, S., Felgueiras, S., & Moura, R. (2024). *The past, present and future of technology in PSP: Preliminary results*. In R. N. A. Fernandes, & P. Machado (Coord.). *40 anos das Ciências Policiais em Portugal* (pp. 389-400), ICPOL

Morgado, S. & Mendes, S. (2016). *O futuro numa década: Os desafios económicos e securitários de Portugal.* 9- 35. https://politeiaonline.pt/article/o-futuro-numa-decada-os-desafios-economicos-e-securitarios-deportugal/

Morgado, S. (2013). *Economics of Public Administration: The right budget to the right public services – The New Management Mythology.* In Z. V. Sovreski, M. Mokryš, Š. Badura, A., Lieskovský (Eds.), Proceedings in 1st Global Virtual Conference Workshop - GV-CONF 2013 (pp. 79-83). Slovakia: EDIS - Publishing Institution of the University of Zilina.

Mozzicafreddo, J. (2017). Como tornar a Administração Pública um serviço Público no contexto de Estados e Sociedades complexas, *Estudos de Administração e Sociedade*, 19-46. https://periodicos.uff.br/revistaeas/article/view/22703/13322

Oliveira M. R. (2024). *eIDAS Qualified services: serviço de validação.* Dissertação de Mestrado Integrado em Engenharia Informática. Universidade do Minho. https://hdl.handle.net/1822/94072

Ongaro, E. (2015). *Administrative reforms in the European Commission and the neo-Weberian model.* In The Palgrave handbook of the European administrative system (pp. 108-123). Palgrave Macmillan UK.

Parisopoulos, K., Tambouris, E., & Tarabanis, K. (2007). *Analyzing and Comparing European eGovernment Strategies.* Informatics and Telematics Institute, Center for Research and Technology Hellas.

Pena, C. A. (2020). *Estudo Comparativo Entre as Aplicações de Assinatura Digital Com O Cartão de Cidadão E a Chave Móvel Digital.* Mestrado em Cibersegurança e Informática Forense. Escola Superior de tecnologia e Gestão. Instituto Politécnico de Leiria.

Pereira, A. L. D. (2017). *Comércio eletrónico (Estudos).* Faculdade de Direita da Universidade de Coimbra. https://egfr.uc.pt/bitstream/10316/44467/1/alexandre%20dias%20pereira%20comercio%20eletronico%202017.pdf

Polícia de Segurança Pública (2002). Plano Estratégico de Sistemas de Informação. Direção Nacional da Polícia de Segurança Pública.

Polícia de Segurança Pública (2013). Visão global de operacionalização da estratégia para as TIC na PSP 2013-2016. Direção Nacional da Polícia de Segurança Pública.

Polícia de Segurança Pública (2025). Estratégia PSP 2025/2027. Direção Nacional da PSP.

Portaria n.º 280/2013, de 26 de agosto, atualizada até à Portaria n.º 266/2024, de 15 de outubro: Regula vários aspetos da tramitação eletrónica dos processos judiciais. https://diariodarepublica.pt/dr/legislacao-consolidada/portaria/2013-34581075

Portaria n.º 441/2008 de 9 de maio. Aprova os modelos de cartão de identificação do pessoal da PSP e de beneficiário familiar do subsistema de saúde da PSP (SAD/PSP). https://diariodarepublica.pt/dr/detalhe/portaria/441-2006-659542

Portaria n.º 674/2007, de 5 de junho: Centraliza o processo de emissão de notificações decorrentes da aplicação de disposições sancionatórias fixadas pelo Código da Estrada. https://diariodarepublica.pt/dr/detalhe/portaria/674-2007-638160

Portaria n.º 73/2018, de 12 de março, atualizada até à Portaria n.º 6-C/2025, de 6 de janeiro: Define os termos e as condições de utilização do Sistema de Certificação de Atributos Profissionais (SCAP), para a certificação de atributos profissionais, empresariais e

públicos através do Cartão de Cidadão e Chave Móvel Digital. https://diariodarepublica.pt/dr/legislacao-consolidada/portaria/2018-152415463

Portaria n.º 762/2024/2, de 18 de outubro: Autoriza a Polícia de Segurança Pública a assumir os encargos orçamentais relativos à aquisição de serviços de desenvolvimento de software de interoperabilidade entre os sistemas de informação de suporte à atividade dos tribunais e o Sistema Estratégico de Informação da Polícia de Segurança Pública. https://diariodarepublica.pt/dr/detalhe/portaria/762-2024-893675948

Quivy R. & Campenhoudt L. (2005). *Manual de Investigação em Ciências Sociais.* 4. ed. Gradiva.

Ravesteyn, P., & Ongena, G. (2019). *The Role of e-Leadership in Relation to IT Capabilities and Digital Transformation.* https://doi.org/10.33965/is2019_201905L022

Regulamento (EU) n.º 2019/1157, de 20 de junho: Visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1157&from=ES

Regulamento (UE) n.º 2024/1183, de 11 de abril: Altera o Regulamento (UE) 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401183

Regulamento (UE) n.º 2024/903, 13 de março: Estabelece medidas para um elevado nível de interoperabilidade do setor público em toda a União (Regulamento Europa Interoperável). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400903

Regulamento (UE) n.º 910/2014, de 23 de julho: Relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910

Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro: Aprova a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o respetivo Plano de Ação Transversal para a legislatura (2021). https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/131-2021-171096337

Resolução do Conselho de Ministros n.º 2/2018, de 5 de janeiro: Procede à revisão do Regulamento Nacional de Interoperabilidade Digital. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/2-2018-114457664

Resolução do Conselho de Ministros n.º 207/2024, de 30 de dezembro: Aprova a Estratégia Digital Nacional e o respetivo modelo de governação. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/207-2024-901536081

Resolução do Conselho de Ministros n.º 34-B/2023, de 20 de abril: Prorroga o mandato da Estrutura de Missão Portugal Digital. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/34-b-2023-212137683

Resolução do Conselho de Ministros n.º 42/2015, de 19 de junho: Determina a adoção preferencial da Plataforma de Interoperabilidade da Administração Pública (iAP) na troca de informação entre serviços e organismos da Administração Pública, e aprova o regime de utilização e os níveis de serviço iAP. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/42-2015-67540636

Resolução de Conselho de Ministros n.º 98/2020, de 13 de novembro: Aprova a Estratégia Portugal 2030, doravante designada por Estratégia, enquanto referencial principal de planeamento das políticas públicas de promoção do desenvolvimento económico e social do País. https://diariodarepublica.pt/dr/analise-juridica/resolucao-conselho-ministros/98-2020-148444002

Riskasari & Ibrahim, M. A. (2025). The Impact of Electronic Identity Cards and the Digitalization of Certificates on Public Service Effectiveness: A Literature Review. *KnE Social Sciences*, 10(18), 1327-1347.

Rito, C. S.G., Piedade, M.B. & Lucas, E. (2019). *Governo Eletrónico – Assinatura Digital Qualificado. Um Caso de Estudo.* 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal. pp. 1-6. https://doi.org/10.23919/CISTI.2019.8760812

Rito, C. S. G. (2018). Governo Electrónico – *Assinatura digital qualificada.* Caso de Estudo: Comunidade Intermunicipal da Região de Leiria. Escola Superior de Tecnologia e Gestão. http://hdl.handle.net/10400.8/3434

Ruiu, P., Saiu, S., & Grosso, E. (2024). Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics. *Future Internet*, 16(7). https://doi.org/10.3390/fi16070228

Sacramento, E. R., Sardo, S., Miguel, A. F., Caixinha, H. J., & Cortês, C. (2022). Considering the Question of the interoperability. *Páginas A & B*, (18), 120-133 https://doi.org/10.21747/21836671/pag18a7

Silva Júnior, A. L. D., Silva, J. B. D., Gomes, P. J. V., Sandes, W. F., Fernandes, R. N. A., & Machado, P. (2022). *Ciências Policiais: Conceito, Objeto e Método de Investigação Científica.* Instituto Superior de Ciências Policiais e Segurança Interna.

Silva, R.J. (2024). *Ecossistema da Carteira de Identidade Europeia (EUDIW): componente 'Person Identification Data (PID) provider'.* Universidade do Minho.

Siscari, L. A. (2025). *A fiabilidade das provas digitais no processo civil.* (Doctoral dissertation). http://hdl.handle.net/10400.5/99562

Soares, B. F. S. (2022). *Transformação digital na administração pública portuguesa: o impacto das estratégias de inovação, modernização e transformação digital.* http://hdl.handle.net/10400.26/43454

Souza, C. (2018). *Coordenação de Políticas Públicas.* Enap.

Tribunal da Relação de Coimbra (2017). Acordão de 25.11.2017 [Proc.: 3031/16.5T8ACB.C1: "I]. https://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fd1c79a3a5f8292c802581e700559808?OpenDocument

Viana, A. (2021). Transformação digital na administração pública: do governo eletrônico ao governo digital. *Revista Eurolatinoamericana de Derecho Administrativo*, 8(1), 115–136. https://doi.org/10.14409/redoeda.v8i1.10330

Viriato, M. A. C. (2023). *Reflexões de uma década ao serviço da PSP: motivações e expectativas para o futuro.* Dissertação de Mestrado Integrado em Ciências Policiais. http://hdl.handle.net/10400.26/45767

ANEXOS

Anexo 1. Proposta de Cartão Digital da PSP

A presente proposta versa sobre o cartão profissional da PSP, concebido com funcionalidades de autenticação, atributos de identificação digital qualificada (ADQ), bem como capacidades de registo de entradas e de controlo de acessos.

Entendemos, que a via mais eficiente e segura será assentar na infraestrutura existente e certificada pelo Estado português, aproveitando a robustez do CC e CMD. Ambos possuem certificados digitais qualificados, emitidos em conformidade com o eIDAS, garantindo validade legal, autenticidade, integridade da informação e não repúdio, tanto em território nacional como na UE. A grande mais-valia desta abordagem está na gestão dinâmica dos atributos profissionais: através da integração com o sistema de Gestão Integrada de Recursos da PSP (GIRe-PSP), sendo possível atualizar em tempo real a informação relativa a funções e categoria, evitando cartões desatualizados ou dependentes de processos burocráticos morosos.

Do ponto de vista técnico, o cartão funcionaria como um dispositivo multifunções:

AEQ: utilização do SDK do Autenticação.gov para gerar assinaturas digitais no formato XAdES (XML Advanced Electronic Signatures), com suporte a selos temporais (RFC 3161), reforçando a validade jurídica.; Autenticação forte em sistemas críticos: combinação de PIN + middleware como segundo fator de autenticação, garantindo o princípio de "defesa em profundidade"; Controlo de acessos físicos: autenticação para entrada em zonas de segurança através de NFC/contactless, com protocolos criptográficos de desafio-resposta baseados em certificados; Registo de assiduidade e ponto: integração direta com os sistemas internos da PSP, eliminando redundâncias e garantindo rastreabilidade e não repúdio no registo de presença.

Requisitos de integração técnica:

Para tornar o cartão plenamente funcional, deverá ser estabelecido um protocolo institucional entre PSP e AMA/ARTE, entidade responsável pela disponibilização do middleware e SDK oficiais do Autenticação.gov.

A aplicação da PSP deverá comunicar com o cartão (através de contacto físico, via leitor ou via NFC, com CAN + PIN) usando o middleware PTEID.

Este inclui: PTEID Middleware: permite o uso das bibliotecas para operações de autenticação e assinatura;

PTEID CMDSignatureClient: cliente específico para assinatura qualificada via CMD, com suporte a XAdES, com ou sem carimbo temporal;

PTEID SDK: bibliotecas que expõem APIs em várias linguagens (C/C++, Java, .NET, Python) para integração direta com aplicações corporativas, aceitando chamadas para ambientes de pré-produção e produção mediante configuração (por exemplo, PTEID_Config).

Fluxo típico de assinatura com atributos profissionais:

O utilizador insere o cartão no leitor ou aproxima via NFC;

A aplicação policial (GIVERH ou SEI) consulta os certificados disponíveis;

O sistema solicita o PIN qualificado ao utilizador;

O SDK gera a AEQ no formato XAdES, associando os atributos profissionais (categoria funcional, unidade orgânica);

A assinatura é validada e registada, podendo incluir selo temporal para assegurar validade prolongada.

Pré-requisitos técnicos:

Sistemas operativos compatíveis: Windows, macOS ou Linux;

Instalação obrigatória do middleware oficial[7]:

SDK Autenticação.gov[8]:

Benefícios estratégicos: Este modelo garante não só a uniformização da identidade digital dos agentes policiais, como também permite alinhar com as diversa estratégias da PSP (EPSP 23/25 e o PESI2).

[7] Autenticação.gov – CC Aplicações
[8] Manual SDK