POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Tratamento e Proteção de Dados na Emergência Pré-Hospitalar

Projeto de Mestrado em Cibersegurança e Informática Forense

Tiago Filipe Almeida Monteiro

Leiria, julho de 2025

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Tratamento e Proteção de Dados na Emergência Pré-Hospitalar

Projeto de Mestrado em Cibersegurança e Informática Forense

Tiago Filipe Almeida Monteiro

Projeto de Mestrado realizado sob a orientação do Professor Doutor Rui Pedro Charters Lopes Rijo e apresentado à Escola Superior de Tecnologia e Gestão de Leiria para obtenção do grau de Mestre.

Leiria, julho de 2025

You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk.

Kevin Mitnick

Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Publicação de artigo

Os resultados do presente projeto, deram origem a um artigo científico intitulado "*Data Processing and Protection in Pre-Hospital Emergency Care*" e submetido para publicação, a dia 15 de junho de 2025, na conferência "*3rd International Conference on Intelligent Computing, Communication, Networking and Services* (ICCNS2025)", estando-se a aguardar a notificação oficial de aceitação a 10 de julho do mesmo ano.

O artigo pode ser consultado na íntegra no Apêndice F.

Agradecimentos

Um projeto académico é uma longa viagem, que inclui uma trajetória permeada por inúmeros desafios, tristezas, incertezas e muitos percalços pelo caminho, mas apesar disso, reúne contributos de várias pessoas, indispensáveis para encontrar o melhor rumo em cada momento da caminhada. Concluir esta fase da minha vida só foi possível com o apoio, energia e força de várias pessoas, a quem dedico especialmente esta conquista.

Ao meu orientador, Professor Doutor Rui Rijo, que sempre acreditou no tema, agradeço a orientação exemplar pautada por um elevado e rigoroso nível científico, um interesse permanente e fecundo, uma visão crítica e oportuna, um empenho inexcedível e saudavelmente exigente, os quais contribuíram para enriquecer, com grande dedicação, passo a passo, todas as etapas subjacentes ao trabalho realizado.

Expresso também a minha enorme gratidão e reconhecimento a todos os professores do regime diurno do curso de Cibersegurança e Informática Forense, pelos conhecimentos e competências que me transmitiram ao longo deste Mestrado, contribuindo na elaboração deste projeto. A constante simpatia e disponibilidade, e o notável nível de literacia que possuem, permitem não só elevar o curso e a escola a um patamar alto de excelência, como também formar bons profissionais de Cibersegurança em Portugal.

Agradeço ainda aos meus colegas de curso, que tive o prazer de conhecer na bela cidade de Leiria, pelo apoio e motivação que ajudou a tornar este Mestrado uma válida e agradável experiência de aprendizagem, e ainda aos meus amigos mais próximos pela solidariedade e capacidade de distração essencial na defesa dos momentos stressantes.

Aos meus pais, avó Isabel e querido avô Carlos, o meu sincero apreço pelo amor e apoio incondicional que contribuiu para o término deste percurso. A exigência e preocupação característica dos familiares são fundamentais para manter o foco e a confiança no objetivo.

A todos os meus colegas Bombeiros e demais profissionais de emergência e socorro pré-hospitalar que colaboraram no presente estudo, o meu sincero e honesto agradecimento pela contribuição no sucesso deste trabalho.

Por fim, um sentido agradecimento a todas as restantes pessoas que, de forma direta ou indireta, contribuíram para a concretização deste projeto, estimulando-me intelectual e emocionalmente.

Resumo

Diariamente, milhares de profissionais em emergência pré-hospitalar lidam com diversos dados pessoais e clínicos, informações sensíveis que podem ser alvos para agentes maliciosos. A segurança no tratamento e proteção desses dados é, portanto, essencial para evitar divulgações não autorizadas e proteger a privacidade das vítimas, mantendo a confiança nos serviços de socorro e cumprindo as exigências legais em vigor.

Nesse sentido, o presente relatório descreve o desenvolvimento de um estudo que não só analisa o enquadramento normativo aplicável ao contexto de emergência pré-hospitalar, como também avalia o nível de consciencialização de uma amostra de profissionais da área relativamente à proteção e ao tratamento de dados de saúde.

Desta forma, o principal objetivo deste trabalho é perceber os direitos e deveres das vítimas e das equipas de socorro, antes, durante e após a prestação de cuidados urgentes, através da sintetização e análise do extenso e específico quadro normativo europeu e português associado a este tema, e da realização de um caso de estudo prático.

Assim, este relatório aborda diversos aspetos, incluindo os trabalhos existentes relacionados, os tipos de serviços e de dados presentes numa operação de emergência médica, a legislação e regulamentação cabível, as dificuldades dos profissionais no terreno, as garantias legais dadas aos titulares dos dados, a metodologia usada no caso de estudo e os resultados obtidos e, por fim, algumas discussões e conclusões acerca do trabalho realizado.

Palavras-chave: Emergência pré-hospitalar, Dados de saúde, Privacidade, Legislação, Consciencialização

Abstract

Every day, thousands of pre-hospital emergency professionals handle various personal and clinical data, sensitive information that can be targeted by malicious agents. The security in processing and protecting these data is, therefore, essential to prevent unauthorized disclosures, protect the privacy of victims, maintain trust in emergency services, and comply with the legal requirements in force.

In this context, this report describes the development of a study that not only analyzes the regulatory framework applicable to the pre-hospital emergency context but also assesses the level of awareness of professionals in the field regarding the protection and handling of health data.

Thus, the main objective of this work is to understand the rights and duties of victims and rescue teams, before, during, and after the provision of urgent care, through the synthesis and analysis of the extensive and specific European and Portuguese regulatory framework associated with this topic, and by the implementation of a practical case study.

This report covers various aspects, including existing related studies, the types of services and data involved in a medical emergency operation, applicable legislation and regulation, the challenges faced by professionals in the field, the legal guarantees provided to data subjects, the methodology used in the case study and the results obtained, and finally, discussions and conclusions about the work carried out.

Keywords: Pre-hospital emergency, Health data, Privacy, Legislation, Awareness

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

AEM	Ambulância de Emergência Médica
AR	Assembleia da República
AS	Ambulância de Socorro
CDF	Carta dos Direitos Fundamentais
CE	Conselho da Europa; Comissão Europeia
CEDH	Convenção Europeia dos Direitos do Homem
CNPD	Comissão Nacional de Proteção de Dados
CODU	Centro de Orientação de Doentes Urgentes
COAZR	Comando Operacional dos Açores
COMDR	Comando Operacional da Madeira
CSIRT	*Computer Security Incident Response Team*
CVP	Cruz Vermelha Portuguesa
DAE	Desfibrilhador Automático Externo
DNS	*Domain Name System*
DPO / EPD	Encarregado de Proteção de Dados
DUDH	Declaração Universal dos Direitos do Homem
EEDS	Espaço Europeu de Dados de Saúde
EHR / RSE	*Electronic Health Record*
ENB	Escola Nacional de Bombeiros
EU / UE	União Europeia
GEM	Gabinete de Emergência Médica
GNR	Guarda Nacional Republicana
GPS	*Global Positioning System*
GSGS	Gabinete do Secretário de Estado da Saúde
HIPAA	*Health Insurance Portability and Accountability Act*
HSPAMI	*Healthcare Security Practice Analysis, Modeling and Incentivization*
IA / AI	Inteligência Artificial
ITEAMS	*INEM Tool for Emergency Alert Medical System*
INEM	Instituto Nacional de Emergência Médica
ISO	*International Organization for Standardization*
LADA	Lei do Acesso aos Documentos Administrativos

LPD	Lei de Proteção de Dados
MEM	Motociclo de Emergência Médica
NIS / SRI	*Network and Information Security*
NTNU	*Norwegian University of Science and Technology*
NU	Nações Unidas
OCDE	Organização para a Cooperação e Desenvolvimento Económico
PEM	Posto de Emergência Médica
PER	Posto de Emergência Reserva
PIA / AIPD	*Privacy Impact Assessment*
PME	Pequenas e Médias Empresas
PSP	Polícia de Segurança Pública
RGPD	Regulamento Geral de Proteção de Dados
SBV	Suporte Básico de Vida
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	Sistema Integrado de Emergência Médica
SIADEM	Sistema Integrado de Atendimento e Despacho de Emergência Médica
SIV	Suporte Imediato de Vida
SNS	Sistema Nacional de Saúde
SPMS	Serviços Partilhados do Ministério da Saúde
TAS	Tripulante de Ambulância de Socorro
TAT	Tripulante de Ambulância de Transporte
TEPH	Técnico de Emergência Pré-Hospitalar
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias da Informação e Comunicação
TIP	Transporte Inter-Hospitalar Pediátrico
UCC	Unidade de Cuidados Continuados
UMIPE	Unidade Móvel de Intervenção Psicológica de Emergência
UNESCO	Organização das Nações Unidas para Educação, Ciência e Cultura
USA / EUA	Estados Unidos da América
USF	Unidade de Saúde Familiar
VMER	Viatura Médica de Emergência e Reanimação
VMIR	Viaturas Médicas de Intervenção Rápida

1. Introdução

Durante grande parte do século XX, os dados de saúde dos pacientes eram registados e armazenados em papel, mantidos em arquivos físicos dentro de hospitais e clínicas e acessíveis apenas por um grupo restrito de profissionais de saúde. Embora esta forma tradicional de registo impusesse limites à eficiência e à partilha de informação, a sua natureza física oferecia uma proteção implícita, reduzindo o risco de acessos não autorizados.

Contudo, com o avanço das tecnologias de informação e o crescente valor associado à privacidade dos dados, a preocupação com a segurança e proteção de dados de saúde foi ganhando força, especialmente entre entidades governamentais e reguladoras. Atualmente, proteger a privacidade dos dados de saúde é reconhecido como um direito fundamental dos indivíduos, e o seu tratamento incorreto pode ter consequências legais e éticas significativas.

Nos últimos anos, diversos avanços foram feitos no sentido de estabelecer um quadro normativo mais rigoroso para o tratamento de dados pessoais, principalmente no setor da saúde. Essas alterações refletem uma preocupação crescente com a segurança e a privacidade das informações pessoais, impondo responsabilidades tanto a nível institucional quanto individual. O objetivo principal dessas normas é garantir que os dados sejam recolhidos, armazenados e utilizados de maneira ética e segura, protegendo o direito à privacidade dos pacientes e assegurando que as informações sejam usadas exclusivamente para finalidades legítimas e com o devido consentimento. Com essas diretrizes, a responsabilidade dos profissionais de saúde e das instituições de prestar cuidados seguros e respeitar a confidencialidade dos dados foi significativamente ampliada, acompanhada de uma fiscalização mais rigorosa por parte das entidades reguladoras.

No entanto, o contexto de emergência e socorro pré-hospitalar impõe desafios específicos para a aplicação rigorosa dessas normas. Nesses cenários, os profissionais - como Técnicos de emergência pré-hospitalar e Bombeiros - precisam de tomar decisões rápidas e informadas que dependem de conhecimento e de acesso a dados pessoais e clínicos das vítimas. Este tipo de intervenção, muitas vezes em ambientes instáveis e imprevisíveis, limita o controlo sobre a privacidade e a proteção das informações dos pacientes, o que torna difícil, na prática, a total conformidade com os requisitos de proteção de dados. Em Portugal, o número de chamadas de emergência recebidas pelos Centros de Orientação de Doentes Urgentes (CODU) através do número europeu de socorro (112) aumentou

significativamente, passando de 500 mil chamadas anuais em 2001 (Barros *et al.*, 2019) para mais de 1.5 milhões de chamadas anuais em 2023. Destas últimas, um total de 1.415.455 casos resultam em intervenção direta no local por parte de acionamento de meios de emergência médica (INEM, 2024). Este volume de atendimentos reflete a frequência com que dados sensíveis de vítimas precisam de ser manuseados, aumentando a exposição a riscos, mesmo que em muitos casos esses dados ainda sejam registados em papel e não em sistemas digitais.

Apesar do uso de registos em formato físico ainda ser uma prática comum, especialmente em cenários pré-hospitalares onde a tecnologia nem sempre está disponível ou viável, a importância da proteção de dados não é menos relevante. A gestão e o armazenamento seguro desses documentos são cruciais, já que informações confidenciais podem facilmente ser expostas acidentalmente ou indevidamente. Neste contexto, a conscientização dos profissionais que atuam em operações de socorro torna-se essencial para garantir que as informações das vítimas são tratadas com o devido cuidado, mesmo em condições adversas.

Desta forma, analisar as formas de tratamento e de proteção de dados na emergência pré-hospitalar torna-se essencial para identificar lacunas e desenvolver práticas que garantam um equilíbrio entre a rapidez de resposta e a segurança dos dados. Este estudo visa, assim, compreender os desafios enfrentados pelos profissionais de emergência médica, explorar as suas perceções sobre as responsabilidades impostas pela legislação e ajudar na identificação de abordagens que permitam melhorar o cumprimento das normas sem comprometer a qualidade e a prontidão do atendimento. Pretende-se assim que a compreensão dos requisitos legais enquadrados ao contexto específico das emergências médicas contribua significativamente para proteger os direitos dos cidadãos e promover a confiança pública nos serviços de socorro.

1.1. Contextualização do projeto

Este trabalho, intitulado "Tratamento e proteção de dados na emergência pré-hospitalar" insere-se na Unidade Curricular de Projeto do curso de Mestrado em Cibersegurança e Informática Forense, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, que tem como objetivo proporcionar aos alunos a oportunidade de desenvolvimento de um trabalho individual e original nas áreas de Cibersegurança e/ou computação forense.

A importância deste estudo, maioritariamente realizado em ambiente académico e de investigação, vai para além da simples aquisição e aplicação de conhecimentos técnicos e práticos. Torna-se ainda uma oportunidade para que os alunos desenvolvam competências como a produção escrita, a pesquisa e citação de bibliografia e *webgrafia* de diferentes fontes de informação, a análise crítica de trabalhos relacionados, a adoção de metodologias de trabalho, a discussão de resultados, a resolução de problemas, entre outras capacidades que são altamente valorizadas no mercado de trabalho atual.

Além disso, este trabalho permite principalmente que os alunos apliquem alguns dos conhecimentos adquiridos ao longo do primeiro ano letivo e ainda obtenham outros específicos na área em que o tema escolhido se insere, abrindo portas a novas competências e experiências.

1.2. Motivação à escolha do tema

A primeira etapa de realização de uma dissertação, tese ou projeto académico debate-se com a escolha do tema a abordar. Como tal, a decisão para a seleção do assunto deste estudo foi demorada e baseou-se na distinção de aspetos preferenciais e não preferenciais entre a lista de temas previamente elaborada pelo autor.

Assim, a motivação para a realização deste projeto decorreu de uma combinação de fatores pessoais e académicos. No decorrer do Mestrado em que este trabalho se insere, o autor apercebeu-se que o tema da proteção de dados pessoais foi abordado de forma limitada durante o curso, talvez devido ao facto de esta ser cada vez mais uma área de especialização do domínio do Direito. Este facto gerou uma curiosidade natural para a exploração mais profunda dos princípios, regulamentos e práticas que envolvem a segurança e a privacidade dos dados, principalmente num contexto tão relevante e sensível quanto o da saúde. A importância dos dados pessoais é um tema central na Cibersegurança, mas o seu tratamento seguro em ambientes de emergência ainda é, em muitos casos, uma área em que se verifica a necessidade de maior clareza e normatização. Esta lacuna académica foi, portanto, um dos principais impulsionadores deste projeto, incentivando à investigação e à aquisição de conhecimentos específicos que complementem o que foi visto ao longo do curso.

Além disso, a experiência profissional do autor como bombeiro voluntário influenciou significativamente a escolha e o direcionamento do projeto. No seu tempo livre, lida frequentemente com situações de emergência pré-hospitalar, onde o acesso a informações

pessoais e de saúde das vítimas é muitas vezes necessário e inevitável. Estas situações expõem, em primeira mão, a importância e os desafios da proteção de dados, uma vez que o ambiente de emergência exige rapidez e eficiência, o que por vezes dificulta a aplicação estrita das normas de privacidade. Por esse motivo, sentiu-se a necessidade de explorar como a proteção de dados pode ser integrada eficazmente neste contexto específico, permitindo que os profissionais desta área possam manter altos padrões de confidencialidade e segurança no tratamento da informação, mesmo em condições adversas.

Assim, este projeto representa não apenas uma oportunidade de aprofundar conhecimentos teóricos e regulamentares, mas também um esforço para conciliar a teoria com a prática. Esta motivação pessoal e académica, aliada à relevância prática do tema, fortalece o empenho em contribuir com um trabalho que se espera ser de utilidade para a área e para o futuro desempenho profissional do autor.

1.3. Definição de objetivos

A definição inicial de objetivos é uma das principais fases que contribuem para o sucesso de qualquer projeto, uma vez que orienta cada etapa do estudo e assegura que todas as questões relevantes sejam exploradas de forma organizada e eficiente.

Desta forma, quanto às metas do projeto escolhido, a proposta teve como principais objetivos:

- Explorar conceitos essenciais à compreensão do tema da proteção de dados no contexto de emergência pré-hospitalar, como dados pessoais, emergência, socorro pré-hospitalar e outros termos-chave;
- Identificar o tipo de dados recolhidos durante operações de emergência, bem como os métodos de recolha, armazenamento e eventual partilha dessas informações;
- Analisar as obrigações legais impostas por códigos de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD), especificamente aplicados ao contexto de emergência pré-hospitalar;
- Identificar as obrigações legais dos profissionais e os direitos e deveres dos titulares dos dados à luz do atual quadro normativo português e europeu;
- Avaliar o nível de consciencialização de uma amostra de profissionais de emergência sobre o tratamento e a proteção de dados, através de um inquérito;

- Avaliar as práticas de proteção e privacidade de dados adotadas pelas equipas de emergência no terreno;
- Identificar os desafios práticos na aplicação das normas em situações de emergência;
- Compreender o impacto e as implicações éticas que a legislação acarreta para as operações de socorro.

Assim, o principal foco deste projeto concentrou-se em explorar e concluir a totalidade dos objetivos anteriormente impostos, garantindo assim uma análise completa, realista e fundamentada do tema em questão.

1.4. Pertinência do estudo

Tal como abordado no início do presente capítulo, a pertinência deste estudo relaciona-se ao facto da crescente importância da proteção de dados pessoais e ao impacto que esta área tem nas operações de socorro pré-hospitalar.

Em situações de emergência, os socorristas frequentemente acedem a informações sensíveis das vítimas, como dados de saúde e de identificação, que são essenciais para o sucesso do atendimento. Contudo, este acesso levanta sérias questões de privacidade e segurança, uma vez que, apesar da urgência, estas informações devem ser protegidas conforme estipulado por regulamentações atuais. O estudo aborda, portanto, a necessidade de conciliar a eficiência no atendimento com o cumprimento das obrigações legais de proteção de dados, promovendo práticas que assegurem a privacidade dos cidadãos, mesmo em contextos de urgência.

A relevância deste trabalho destaca-se também pelo fato de que a proteção de dados no contexto de emergência pré-hospitalar é, ainda, uma área pouco explorada e debatida. Ainda que, desde o ano de 2021, algumas entidades, como o INEM e a ENB, tenham desenvolvido esforços para que se aumente a consciencialização e formação dos profissionais de emergência médica acerca deste tema, o avanço das tecnologias e o aumento e a atualização das legislações existentes cresce igualmente, aumentando a preocupação sobre como os dados das vítimas são tratados e armazenados em momentos críticos. Esta investigação pretende preencher algumas das lacunas existentes, proporcionando uma visão clara sobre as práticas atuais e as dificuldades enfrentadas pelas equipas de emergência na aplicação das normas de proteção de dados.

Além disso, a pertinência deste projeto é reforçada pelo impacto que este pode ter na formação e sensibilização dos profissionais de emergência. Ao investigar o nível de consciencialização destes intervenientes sobre a proteção de dados, este estudo contribui para identificar áreas onde é necessário reforçar o conhecimento e a prática de boas condutas de privacidade e segurança. Tal sensibilização é fundamental para assegurar que os dados sejam manuseados de forma responsável e que a confiança nos serviços de emergência seja mantida, reforçando a legitimidade e a credibilidade destas instituições governamentais e humanitárias perante o público.

Finalmente, o estudo assume particular importância numa época em que a sociedade exige transparência e rigor no tratamento de dados pessoais. Este projeto oferece, assim, uma análise das obrigações legais e éticas que envolvem o manuseio de informações sensíveis no contexto de emergência, promovendo um melhor entendimento dos direitos dos cidadãos e das responsabilidades dos profissionais. Ao contribuir com esta reflexão, pretende-se que o estudo ajude a alinhar as necessidades operacionais das equipas de socorro com a privacidade dos indivíduos, demonstrando que, mesmo em situações de urgência, é possível adotar práticas de proteção de dados que respeitem a legislação e as expectativas de segurança da sociedade.

1.5. Planeamento do trabalho

Estabelecer um rigoroso planeamento de trabalho é fundamental para garantir que todas as atividades sejam realizadas dentro do prazo esperado. A equilibrada e correta calendarização das tarefas a realizar durante o projeto ajuda a evitar sobrecarga de trabalho em momentos específicos e a garantir que o estudo esteja pronto para entrega na data esperada e com a qualidade que se propõe desde a fase inicial.

Assim, a criação de uma tabela de *Gantt* torna-se essencial para o planeamento e a gestão eficaz de projetos, uma vez que este tipo de gráfico permite visualizar de forma clara e organizada todas as etapas de trabalho, desde a conceção até à conclusão. Seguir esta *timeline* ajuda a garantir que todas as tarefas sejam realizadas dentro do prazo estipulado, evitando atrasos e sobreposições de atividades. Além disso, esta abordagem estruturada é fundamental para manter o foco, identificar possíveis problemas com antecedência e assegurar o cumprimento dos objetivos inicialmente estabelecidos.

Nesse sentido, a Figura 1 ilustra uma tabela de *Gantt* que abrange o período de setembro até junho (correspondente a cerca de um ano letivo) e detalha as principais tarefas necessárias para a realização deste projeto.

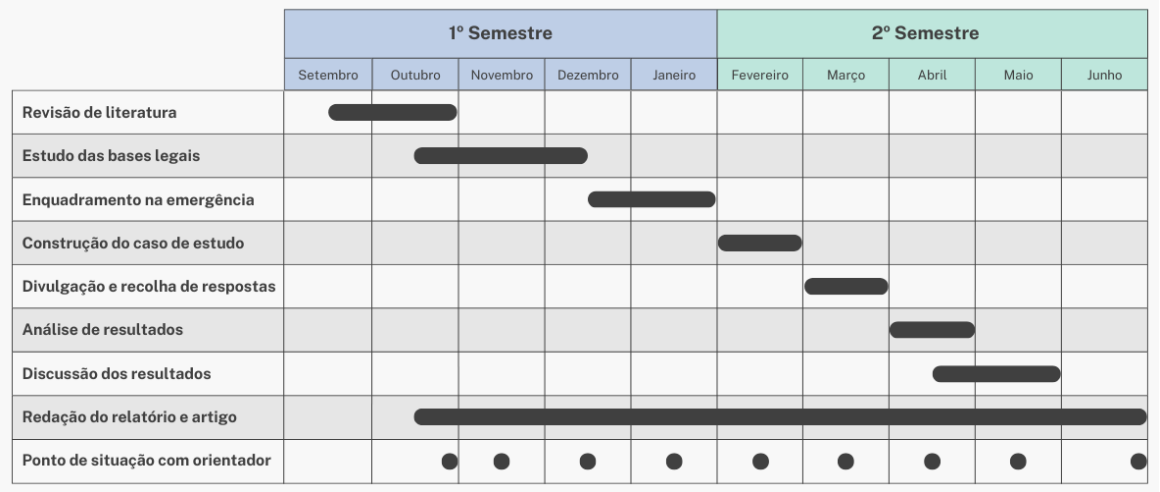


Figura 1 – Gestão das tarefas em função do tempo

Assim, no término do mês de Setembro, o projeto iniciou-se com um período de cerca de 1 mês e meio destinado à realização da revisão de literatura. Esta etapa foi essencial para procurar e analisar trabalhos académicos e de investigação que estavam alinhados com os tópicos a serem abordados neste estudo.

De seguida, e durante cerca de dois meses, realizou-se o estudo da regulamentação que compõem o atual quadro normativo associado à proteção de dados de saúde. Após este último, seguiu-se um período temporal que será investido no enquadramento do estudo anterior ao contexto da emergência e socorro pré-hospitalar. O tempo despendido nesta e na anterior etapa justificou-se dado o nível de especificidade associado ao objetivo.

No começo do 2º Semestre previu-se o avanço do projeto para a fase prática do estudo, iniciando a construção do questionário online a ser distribuído pelos profissionais. Associada a esta fase esteve a divulgação desse mesmo inquérito junto de entidades e grupos-alvo, que permitiu a obtenção de uma amostra significativa de resultados.

Tendo-se aguardado um período de 1 mês após a partilha das questões, deu-se a etapa de análise e discussão das respostas obtidas, começando pela caracterização da aderência e terminando na avaliação do nível de consciencialização dos profissionais relativamente ao tema em estudo.

Além disso, ao longo de todo o período letivo realizou-se a escrita da documentação. Esta abordagem evitou que a redação fosse deixada para o final, o que poderia resultar em perda de qualidade e rigor. Assim, pretendeu-se que a revisão fosse realizada idealmente logo após a conclusão de cada novo capítulo, permitindo ajustes e melhorias contínuas, e garantindo que a documentação estivesse sempre atualizada e coerente. A escrita de um artigo sobre o trabalho realizado incluiu-se também nos objetivos para este projeto.

Por fim, acreditou-se ser essencial a realização de pontos de situação regulares com o orientador, uma vez que essas reuniões periódicas eram fundamentais para manter todos os envolvidos informados sobre o progresso do projeto, discutir dificuldades encontradas e receber feedback sobre o trabalho desenvolvido. Essa comunicação constante ajudou a alinhar expectativas, corrigir rumos se necessário, e assegurar que o projeto se mantinha no caminho certo para atingir os objetivos propostos. Como tal, o primeiro encontro estabeleceu-se no final do mês de outubro, seguindo-se várias reuniões mensais que pretenderam coincidir com cada uma das tarefas do projeto.

Em suma, ainda que este cronograma permitisse a flexibilidade suficiente para a correção de possíveis percalços, pretendeu-se segui-lo de forma rigorosa para que se garantisse o sucesso do projeto, através de uma gestão eficiente do tempo e dos recursos, e da garantia de entrega de resultados de alta qualidade.

1.6. Estrutura do relatório

Quanto à estrutura, este documento encontra-se organizado em oito capítulos.

Após esta introdução, inicia-se o segundo capítulo, que apresenta uma revisão das principais conclusões de diferentes trabalhos que se encontram, de alguma forma, relacionadas ao tema deste projeto.

Já o terceiro capítulo pretende dar a conhecer a área profissional abordada: a emergência pré-hospitalar. Com tal, são abordados alguns temas como os serviços prestados, os meios tecnológicos disponíveis e utilizados, o tipo de dados recolhidos e as situações de uso dessas informações, com o intuito de prover algum contexto sobre esta atividade aos leitores.

De seguida, no capítulo quarto abordam-se todos os relevantes regulamentos e legislações que, de alguma forma, possuem alguma matéria relacionada ao contexto da proteção de dados na emergência pré-hospitalar, seja através da definição de conceitos ou

da descrição de normas legais. Todos esses recursos foram explorados e divididos tendo em conta a sua abrangência: europeia ou nacional.

O quinto capítulo propõe falar sobre o enquadramento da legislação anteriormente estudada em relação à realidade dos profissionais de emergência e socorro. Esta contextualização foi útil para que se pudesse compreender as obrigações dos socorristas e os direitos e deveres das vítimas, titulares dos dados.

É no sexto capítulo que se implementou o caso de estudo associado ao projeto. Numa fase inicial foi estudada a metodologia a adotar, tendo em conta a melhor estratégia/método de pesquisa, a caracterização da população e da amostra expectável, o instrumento de recolha de dados utilizado e os procedimentos de pré-teste. Após a construção e divulgação desse inquérito, o mesmo capítulo descreve ainda a amostra obtida, avalia o nível de consciencialização dos profissionais e identifica os riscos e desafios encontrados através das respostas adquiridas.

No capítulo sétimo é realizada uma discussão do caso de estudo através da interpretação dos resultados em relação à revisão de literatura, com vista à validação de aspetos em comum, da identificação de implicações e dificuldades da implementação da regulamentação na prática pré-hospitalar e, por fim, da exploração de possíveis recomendações para profissionais e respetivas entidades.

Por último, o oitavo capítulo, denominado “Conclusões”, foca-se em alguns assuntos relevantes tais como recapitulação de objetivos inicialmente estabelecidos, resultados e contribuições obtidos, obstáculos e dificuldades sentidas, e possíveis melhorias a acrescentar ao projeto realizado.

2. Revisão da literatura

Este capítulo apresenta a revisão de literatura, suportada por estudos que fornecem uma visão abrangente sobre as abordagens e práticas existentes na proteção de dados em serviços de emergência. Esta análise visa identificar as contribuições, limitações e tendências desses trabalhos, de modo a enquadrar a relevância e os objetivos do estudo proposto.

2.1. Metodologia de pesquisa

O estabelecimento de critérios claros para a pesquisa de literatura revela-se fundamental para assegurar que qualquer revisão seja relevante e robusta.

Nesse sentido, numa fase inicial, a seleção de literatura envolveu a identificação do propósito de cada potencial fonte, analisando-as sob três diferentes aspetos:

- **Conceito:** Representa as áreas principais do problema, incluindo a ideia principal, o campo de interesse e o tópico que se pretende investigar. No contexto deste estudo, o conceito centra-se na proteção de dados em emergências pré-hospitalares (Morgado, 2024);
- **Contexto:** Refere-se à delimitação da área onde o conceito é aplicado. Inclui onde o conceito surge, onde é aplicado, quem está envolvido, e outras formas de relacionar o conceito. No caso em estudo, o contexto engloba as situações específicas de socorro pré-hospitalar onde ocorre o tratamento de dados (Morgado, 2024);
- **Perspetiva:** Define a lente através da qual o conceito será examinado dentro do contexto, ou seja, clarifica a intenção geral da pesquisa, como a análise das obrigações legais ou as práticas de proteção de dados de saúde em ambientes de emergência (Morgado, 2024).

Após a compreensão e identificação destes conceitos, seguiu-se a seleção das fontes de pesquisa. Para tal, uma variedade de ferramentas digitais e manuais foram adotadas de forma a otimizar e automatizar a identificação de literatura relevante ao tema em estudo.

No *Google Scholar*, ou Google Académico, as pesquisas foram efetuadas usando diferentes *queries* como *(intitle: "review" | intitle: "survey") "prehospital emergency care"* ou *("data protection" | "privacy") "emergency medical services" review*. Recorrendo aos

filtros disponíveis, foi ainda possível configurar a pesquisa para visualizar preferencialmente publicações com um máximo de 10 anos. Esta abordagem proporcionou uma ampla cobertura de documentos, apesar de alguns dos trabalhos apresentarem credibilidade questionável (Morgado, 2024).

Simultaneamente, as pesquisas em bases de dados bibliográficas como o *Scopus*, *b-on*, *JSTOR*, *EBSCO*, *ResearchGate*, *Litmaps*, *Academia*, *IEEE Explore*, entre outros, ofereceram vantagens significativas como a possibilidade de pesquisa por título, resumo e palavras-chave, além da existência de filtros mais precisos como faixa de publicação por ano, nome do autor e área de estudo. De forma intuitiva proporcionam ainda um acesso direto aos resumos dos resultados encontrados, possibilitando uma melhor análise dos mesmos. Assim, a pesquisa nestas ferramentas resultou numa cobertura mais restrita, porém com publicações de maior credibilidade (Morgado, 2024).

Além destas plataformas, recorreu-se também a ferramentas de inteligência artificial (IA) como *Copilot*, *ChatGPT* e *Undermind*, que permitem uma entrada flexível de dados e apresentam as fontes consultadas. Estas ferramentas revelaram-se úteis no debate e na análise dos resultados obtidos, ainda que enfrentem limitações, tais como a tendência para aceder a fontes genéricas e o risco de interpretarem ou modificarem os dados dos estudos de forma inadequada (Morgado, 2024).

Também as pesquisas em determinados livros ou manuais de entidades como o INEM permitiram consultar informações mais estruturadas e solidificadas, oferecendo uma base confiável para compreender práticas e procedimentos específicos no contexto em estudo.

Após a escolha das fontes de trabalhos, foi realizada a pesquisa de alguns termos-chave cujos resultados obtidos foram filtrados pela relevância do título e local de publicação. Posteriormente, seguiu-se uma avaliação mais detalhada dos resumos para determinar a proximidade com o propósito do estudo e, assim, selecionar os trabalhos mais adequados.

Para garantir a validade e importância das fontes, foram evitados repositórios não verificados, jornais, *blogs* e redes sociais, optando-se por fontes científicas credíveis (Morgado, 2024).

Por fim, a pesquisa deu-se como concluída quando se atingiu a saturação teórica, indicando uma cobertura satisfatória do tema (Morgado, 2024). Esta abordagem estruturada assegurou que a revisão de literatura fosse abrangente e alinhada com os objetivos do estudo,

fornecendo uma base sólida para a discussão subsequente da proteção de dados em contexto de socorro pré-hospitalar.

2.1. Trabalhos relacionados

A análise de trabalhos relacionados ao tema deste estudo é essencial para compreender o estado atual da proteção de dados em diferentes contextos e identificar lacunas que possam ser exploradas. Neste sentido, e tendo em conta os critérios explorados pelo anterior subcapítulo, foram selecionados alguns artigos e relatórios de projetos, dissertações e investigações que abordam temas semelhantes, permitindo uma visão ampla sobre as práticas, desafios e implicações legais associados à proteção de dados pessoais, especialmente em ambientes de saúde e emergência. Desta forma, pretende-se apresentar os pontos mais relevantes de cada trabalho analisado.

No âmbito do Mestrado em Administração Pública, a autora Carina Carvalho desenvolveu uma dissertação cujo tema aborda a proteção de dados pessoais no setor da saúde, com ênfase na aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD) nos cuidados de saúde primários. Numa primeira abordagem, o documento inicia a apresentação da evolução da saúde em Portugal desde a Constituição de 1976 até a implementação do RGPD em 2018. Este marco legal trouxe mudanças significativas na forma como as organizações tratam dados sensíveis, reforçando a segurança, a privacidade e os direitos dos titulares (Carvalho, 2022).

Além disso, destaca-se a também evolução do Sistema Nacional de Saúde (SNS), mostrando como as reformas implementadas ao longo das últimas décadas impactaram a organização e a eficiência do sistema. Os cuidados de saúde primários, essenciais como primeira abordagem ao cidadão, foram aprimorados por meio da criação de unidades funcionais, como as Unidades de Saúde Familiar (USF) e Unidades de Cuidados na Comunidade (UCC), que aumentam a proximidade com os utentes (Carvalho, 2022).

A aplicação do RGPD no setor da saúde é analisada, destacando desafios éticos e práticos relacionados ao tratamento e acesso de dados sensíveis. O relatório aponta que as questões de confidencialidade e privacidade são centrais, especialmente considerando a acessibilidade de informações por múltiplos profissionais de saúde. Exemplos práticos são apresentados, como o esforço das unidades USF Cidade do Lis e UCC Dr. Gorjão Henriques para cumprir os padrões de conformidade com o RGPD (Carvalho, 2022).

Finalmente, o documento enfatiza a importância da boa governança como um pilar para promover equidade e eficiência nos serviços de saúde, além de encerrar com reflexões pessoais da autora. Segundo a opinião pessoal da mesma, a publicação do RGPD fez emergir uma nova preocupação e consciencialização nos profissionais de saúde em matéria de proteção de dados. Os profissionais e, nomeadamente, as instituições tiveram de se adaptar e realizar alterações nos procedimentos internos de forma a dar resposta à nova realidade para evitar violações à lei da proteção de dados pessoais, que pudessem resultar em processos jurídicos. Contudo, toda esta transformação não levou a que as entidades realizassem formação para atualização e aquisição de novos conhecimentos na questão da nova legislação (RGPD) para os profissionais, existindo alguma sensibilização, mas escassa formação em serviço (Carvalho, 2022).

Segundo a análise realizada por este estudo, os dados pessoais em saúde são considerados sensíveis, privados e abrangentes, como descrito no artigo 3º da Lei n.º 12/2005, que refere que a "informação de saúde, incluindo os dados clínicos registados e outros exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa". Anteriormente ao RGPD, o profissional de saúde tinha em consideração o sigilo profissional e o código deontológico da sua área profissional, mas as novas regulamentações vieram aumentar as responsabilidades e/ou a consciencialização da forma como os dados pessoais são tratados, uma vez que reforça o direito do cidadão pelos seus dados e impõe regras mais restritas às entidades que utilizam esses dados (Carvalho, 2022).

A autora defende que a grande problemática na aplicabilidade de legislações como o RGPD refere-se aos pedidos de informação pelos titulares e/ou familiares dos dados pessoais e às obrigações legais que se encontram dependentes. Com frequência, verificou-se o desconhecimento em relação à atuação na questão de proteção de dados pessoais de saúde dos utentes, especificamente em facultar o acesso aos seus dados pessoais que, anteriormente, pensava-se serem institucionais. Além disso, conclui-se que a implementação da legislação não tem sido fácil, principalmente nas entidades públicas, onde os recursos humanos e financeiros são insuficientes e a exigência e complexidade dos regulamentos são diversas, tornando a sua efetivação complexa (Carvalho, 2022).

Numa perspetiva idêntica, o autor Gonçalo Nunes discutiu na sua dissertação de Mestrado em Gestão e Economia da Saúde o tratamento de dados pessoais de saúde à luz do mesmo regulamento abordado pela autora anterior (Nunes, 2019).

Segundo este estudo, a evolução dos direitos fundamentais no Século XX são analisados, destacando os de 3ª geração, como o direito à proteção de dados pessoais e o acesso a documentos administrativos. Esses direitos ganharam força com a globalização e o avanço tecnológico, culminando no Regulamento Geral de Proteção de Dados. Este regulamento substituiu a antiga Diretiva 95/46 e introduziu três pilares principais: novas obrigações para empresas, direitos ampliados aos titulares dos dados e maiores poderes às autoridades reguladoras (Nunes, 2019).

A legislação europeia é também explorada, desde a Declaração Universal dos Direitos Humanos até a adoção do RGPD, um marco que revogou a antiga Diretiva 95/46/CE. Este regulamento introduziu novos princípios, como o "*privacy by design*" e "*privacy by default*", que asseguram maior controlo aos cidadãos sobre os seus dados, e reforçou o papel das autoridades de proteção de dados, como a Comissão Nacional de Proteção de Dados em Portugal (Nunes, 2019).

No contexto da saúde, os dados pessoais, intrinsecamente ligados à privacidade, incluem informações sobre o estado físico ou mental do indivíduo. O RGPD estabeleceu direitos fundamentais como o acesso aos processos clínicos, retificação de dados, direito a ser esquecido, portabilidade, oposição ao tratamento, e preservação da confidencialidade por meio de medidas como pseudonimização[1]. No entanto, existem exceções para o uso de dados em interesse público, como saúde pública e pesquisa científica (Nunes, 2019).

O autor refere ainda que o sigilo profissional dos médicos é obrigatório, mas pode ser quebrado com o consentimento do paciente, em emergências ou para preservar a saúde pública. O tratamento de dados pessoais deve seguir os princípios de licitude, limitação, exatidão, confidencialidade e responsabilidade, garantindo a proteção dos dados enquanto promovem a pesquisa científica, essencial para o avanço médico e social (Nunes, 2019).

Assim, o texto conclui destacando a necessidade de equilibrar a privacidade individual com os benefícios públicos, como o desenvolvimento de novos tratamentos, reconhecendo que a participação dos pacientes na pesquisa clínica é crucial, embora desafiadora, devido à resistência à mudança e às implicações éticas e práticas (Nunes, 2019).

[1] Tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável (SPMS, s.d.).

Com uma abordagem semelhante à pretendida para este projeto, na perspetiva da exploração teórica de conceitos seguida da realização de um caso de estudo prático, o trabalho "Proteção de dados de saúde" de Ana Rio Tinto, desenvolvido no contexto do Mestrado em Gestão de Saúde, aborda a proteção de dados de saúde com foco na perceção e conhecimento do RGPD por parte de administradores hospitalares. Este trabalho está organizado em torno de cinco eixos principais: a evolução histórica do conceito de privacidade, os desafios à confidencialidade, os direitos introduzidos pelo RGPD, as vulnerabilidades tecnológicas e as implicações para a administração hospitalar (Tinto, 2018).

Segundo uma adaptação da autora, a proteção de dados tem uma trajetória histórica significativa, marcada por marcos normativos que estabeleceram as bases para o respeito à privacidade e confidencialidade. Entre os principais acontecimentos históricos destacados, estão a Declaração Universal dos Direitos do Homem e a Convenção Europeia dos Direitos do Homem, que reconheceram a privacidade como um direito fundamental, ainda antes da segunda metade do século XX (Tinto, 2018).

Nos anos seguintes, surgiram diversos avanços como a primeira lei moderna de privacidade na Alemanha (1970) e o *Data Act* na Suécia (1973-1974), considerado a primeira legislação nacional de privacidade. Na década de 80, documentos como as *Guidelines* da OCDE e a Convenção 108 do Conselho da Europa reforçaram a proteção de dados a nível internacional (Tinto, 2018).

Ainda antes do término do século, a importante Diretiva 95/46/CE da União Europeia consolidou a proteção de dados como uma prioridade, e o Tratado de Lisboa, em 2007, aprofundou esse compromisso, estabelecendo bases para o RGPD. Todos estes marcos representam a evolução normativa que veio a culminar na robustez das atuais legislações de proteção de dados (Tinto, 2018).

O RGPD, por sua vez, fortaleceu e harmonizou essas normas na União Europeia, substituindo a Diretiva 95/46/CE e introduzindo inovações significativas, como os direitos ampliados aos titulares dos dados, os deveres dos responsáveis pelo tratamento das informações pessoais e as sanções aplicáveis ao incumprimento das normas (Tinto, 2018).

Para os titulares, incluem-se novos direitos, como o acesso, portabilidade, apagamento e controlo dos dados, que têm implicações diretas para as organizações de saúde, que são obrigadas a criar estruturas de governança e a adotar medidas de segurança como

encriptação, pseudonimização e formação contínua dos profissionais. Assim, o regulamento torna-se um pilar central na garantia da proteção de dados sensíveis, como os de saúde, e impõe padrões elevados para a segurança dos dados (Tinto, 2018).

Além disso, a privacidade e a confidencialidade são contextualizadas desde as origens no Juramento de Hipócrates até às regulamentações mais modernas, sendo a privacidade tratada como um direito fundamental, enquanto a confidencialidade é descrita como um dever ético e legal dos profissionais de saúde. O avanço tecnológico e a digitalização dos dados de saúde são também destacados como desafios para preservar esses direitos, especialmente diante de vulnerabilidades como acessos não autorizados e falhas na segurança (Tinto, 2018).

Outro aspeto relevante abordado é a fragmentação dos dados de saúde devido à descentralização no sistema hospitalar. Essa fragmentação dificulta a implementação de modelos integrados, como o Registo de Saúde Eletrónico (RSE), que visam centralizar as informações de pacientes e permitir um maior controlo pelos titulares. Exemplos como o sistema de saúde da Estônia mostram o potencial de registos centralizados para melhorar a segurança e a eficiência (Tinto, 2018).

Por fim, a autora elabora um estudo prático que pretende aferir o grau de conhecimento dos gestores de organizações de saúde portuguesas acerca das medidas e mecanismos necessários à proteção de informação de saúde dos utentes, no contexto do novo regulamento geral de proteção de dados da UE, e o seu grau de preparação para responder às exigências da aplicação deste diploma jurídico. Nesse sentido, é feita uma apresentação da metodologia de análise quantitativa, baseada na aplicação de questionários via eletrónica, além da descrição dos instrumentos utilizados para a recolha dos dados, a caracterização da amostra, bem como a discussão e tratamento dos resultados obtidos (Tinto, 2018).

O inquérito desenvolvido no referido estudo é composto por diversas questões de escolha múltipla que incidem sobre temas como informações profissionais do inquirido, definições e questões gerais acerca do RGPD, direitos dos titulares e procedimentos considerados obrigatórios para proteção da sua informação, forma como o processo de tratamento de dados deve ser executado e potenciais sanções.

Os resultados obtidos evidenciaram a insuficiência de preparação dos profissionais inquiridos para lidar com as novas exigências. Entre as principais conclusões, destaca-se o

entendimento limitado sobre conceitos essenciais do RGPD, como os direitos dos pacientes (portabilidade e apagamento), técnicas de segurança de dados e procedimentos para avaliação de impacto e notificação de violações. Além disso, foi constatado que poucas unidades hospitalares elevaram a proteção de dados a um nível estratégico, restringindo-se a ações básicas como levantamento de bases de dados e alguns treinamentos pontuais (Tinto, 2018).

Com base nessas lacunas, foram propostas pela autora recomendações práticas para aprimorar a conformidade com a legislação, como a nomeação de um responsável pelo tratamento de dados, a criação de registos de atividades de processamento e a implementação de avaliações de impacto. A necessidade de programas estruturados de formação e sensibilização foi ressaltada como essencial para capacitar os gestores e integrar o RGPD à estratégia organizacional. Este regulamento, com o seu impacto significativo na gestão e proteção de dados de saúde, representa um dos maiores desafios para os administradores hospitalares no futuro próximo (Tinto, 2018).

Na Universidade do Minho, o aluno Francisco Andrade, juntamente com dois coautores do departamento de informática, desenvolveu um documento intitulado "Privacidade e Proteção de Dados nos Cuidados de Saúde de Idosos" que aborda as complexidades e desafios associados ao uso de dados na área da saúde, especialmente focado no atendimento a idosos (Andrade *et al.*, 2011).

O estudo destaca os riscos de violação da privacidade que podem surgir com a implementação de tecnologias de assistência, e aponta que, embora essenciais para fornecer cuidados eficientes, esses sistemas recolhem uma grande quantidade de dados pessoais e sensíveis, o que aumenta o potencial para acessos não autorizados e uso indevido das informações. A partilha de dados entre múltiplos intervenientes, incluindo profissionais de saúde e familiares, sem as devidas medidas de segurança, pode levar a comprometimentos graves da privacidade do paciente (Andrade *et al.*, 2011).

Este estudo tem uma aplicação direta ao contexto pré-hospitalar, onde o uso de equipamentos eletrónicos veículos de emergência é fundamental para o monitoramento e tratamento imediato das vítimas. Esses dispositivos são capazes de recolher e armazenar dados críticos de saúde em tempo real, que, se não forem adequadamente protegidos, podem colocar a privacidade dos titulares dos dados em risco.

Os autores concluem destacando a necessidade crítica de desenvolver estratégias que garantam a eficiência dos cuidados médicos enquanto protegem a privacidade e os dados pessoais, especialmente dos idosos, que são particularmente vulneráveis devido à falta de familiaridade com tecnologias novas. Além disso, enfatizam ainda a importância de um equilíbrio entre tecnologia e ética, com procedimentos que respeitem as leis de proteção de dados e a dignidade dos pacientes. Por fim, recomendam práticas seguras, legislação adequada e consentimento informado como essenciais para preservar a confiança e a integridade dos sistemas de saúde tecnologicamente avançados (Andrade *et al.*, 2011).

Além da comunidade académica, e tendo em consideração os riscos e exigências lançados pelo novos regulamentos e legislações, também as organizações públicas e governamentais têm vindo a desenvolver e publicar diversos documentos orientados ao cumprimento e divulgação da lei. Exemplo dessa partilha é um primeiro guia realizado pelos Serviços Partilhados do Ministério da Saúde (SPMS), E.P.E, que entenderam ser estratégico para o setor da saúde em Portugal a preparação e divulgação junto de todas as entidades de saúde um documento que serve para auxiliar a reflexão e subsequente ação na área da "Privacidade da Informação no Setor da Saúde" (SPMS, s.d.).

O estudo começa por destacar os desafios da transformação digital no setor da saúde, nomeadamente a existência, por vezes, de pouco conhecimento sobre a arquitetura informacional de suporte, nomeadamente no que refere ao armazenamento dos dados dos utentes. Além disso, a entidade autora refere ainda que os dados e informações são partilhados para outros objetivos que não o tratamento direto dos utentes, como em casos de investigação, gestão de saúde pública ou gestão da procura. É ainda referido que os processos de tratamento são operacionalizados através do ecossistema do doente num ambiente de cuidados integrados, no qual todos os prestadores de serviços, têm acesso aos dados das vítimas (SPMS, s.d.).

De seguida, o documento contextualiza juridicamente a proteção de dados no setor da saúde em Portugal, abordando os dados pessoais como quaisquer informações que, direta ou indiretamente, identifiquem uma pessoa singular (o "titular dos dados"), tais como o nome, a morada, o endereço de correio eletrónico, mas também dados relativos a historiais clínicos, historial e características de doenças e perfis de utilizadores/utentes (SPMS, s.d.).

No seguimento dessa contextualização regular, são referidas as obrigações legais associadas ao tratamento de dados pessoais e boas práticas para a adaptação a regulamentos

como o RGPD. Assim, é explorado com detalhe regras gerais de proteção de dados, obrigação de notificação e o controlo prévio da Comissão Nacional de Proteção de Dados, o consentimento, o direito de informação e acesso a dados de saúde, a utilização desses dados para investigação científica, a comunicação de dados e a subcontratação, a implementação de especiais medidas de segurança e, por fim, as consequências do incumprimento (SPMS, s.d.).

Além disso, os SPMS referem ainda que entre as principais medidas exigidas pelo RGPD estão o princípio de "*privacy by design"* e "*privacy by default*", a realização de avaliações de impacto (PIAs) para tratamentos de dados sensíveis, e a nomeação de um Encarregado de Proteção de Dados (DPO) (SPMS, s.d.).

Este guia apresenta ainda uma lista de boas práticas específicas para diferentes perfis, incluindo administradores hospitalares, profissionais de saúde e técnicos de tecnologia da informação (TIC), enfatizando a importância da formação contínua, do engajamento estratégico com a privacidade e da integração de medidas de segurança em todos os níveis organizacionais (SPMS, s.d.).

Por fim, os SPMS reforçam a necessidade de criar um ambiente seguro e transparente no setor da saúde através da apresentação de uma tabela que orienta determinadas recomendações a diferentes entidades, tendo em conta diversos fatores como governança, processos, segurança e direitos (SPMS, s.d.).

Numa outra vertente de referência literária, também o INEM, no seu mais recente manual de Tripulante de Ambulância de Socorro (TAS), dedica uma secção do documento à abordagem da proteção de dados em contexto de emergência médica (INEM *et al.*, 2024).

Neste segmento de texto é abordado o tratamento de informações sensíveis no contexto da prestação de cuidados de emergência pré-hospitalar, destacando a necessidade inevitável da recolha informações pessoais, como nome, idade e histórico médico, para viabilização do atendimento e do registo hospitalar (INEM *et al.*, 2024).

Nos termos do RGPD, o tratamento desses dados, designadamente a recolha ou o registo em suporte próprio, pelos profissionais de saúde que têm acesso à informação, baseia-se no consentimento do titular dos dados, podendo ser prestado mediante um ato positivo inequívoco, desde que livre, específico, explícito e esclarecido, que poderá ser uma declaração escrita ou mediante declaração oral (art.º 4.º do RGPD) (INEM *et al.*, 2024).

É também referido que, durante o processo de prestação de socorro, os dados a que as equipas têm acesso são facultados voluntariamente pelos titulares, cuja finalidade é, não só a prestação de socorro, como também a inscrição no estabelecimento hospitalar de destino do doente, cuja obrigatoriedade é fixada individualmente pelas unidades hospitalares (INEM *et al.*, 2024).

Por outro lado, para prestar cuidados de socorro, é essencial tratar dados de saúde, que incluem informações sobre o estado de saúde de uma pessoa, tanto do passado quanto do presente, como o uso de medicação habitual e históricos médicos, recolhidos durante o atendimento (INEM *et al.*, 2024).

Para situações em que o titular dos dados esteja inconsciente, e por isso, incapaz de manifestar consentimento, o regulamento prevê igualmente a licitude do tratamento, sempre que "o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento" (al. c) do n.º 2 do art.º 9.º do RGPD) (INEM *et al.*, 2024).

O manual destaca ainda que qualquer tratamento só é lícito se for realizado por profissionais sujeitos ao dever de sigilo profissional e desde que devidamente autorizados, mesmo após o termo das respetivas funções (INEM *et al.*, 2024).

Por fim, o documento aborda ainda que o titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, informações sobre o tratamento dos seus dados, e goza ainda de diversos direitos como o de acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição e, remoção do seu consentimento (INEM *et al.*, 2024).

Ainda no âmbito das formações e recomendações conduzidas pelo INEM, também a Rita Abreu Lima, Encarregada de Proteção de Dados (DPO) desta entidade, desenvolveu um trabalho focado no Regulamento Geral sobre a Proteção de Dados, especialmente orientado para profissionais do setor da saúde. Este estudo, inserido sob forma de curso na plataforma Aprender INEM, inicia com a afirmação da autora sobre os atrasos observados na implementação do RGPD no setor da saúde, destacando-se a necessidade de uma adaptação mais eficiente e informada às exigências do regulamento (Lima, 2021).

Durante o início da exposição, a autora faz uma distinção clara entre dados pessoais - como nome, número de cidadão, *e-mail*, e outros atributos que identificam uma pessoa - e

dados pessoais sensíveis, que incluem informações como opiniões políticas, origem racial ou étnica, detalhes sobre a vida sexual e, crucialmente, dados relacionados à saúde. É nesta altura enfatizada a necessidade de um cuidado especial com os dados sensíveis, devido à sua natureza delicada (Lima, 2021).

A formadora aborda ainda o tratamento de dados como sendo qualquer operação realizada sobre dados pessoais, seja ela a recolha, armazenamento, consulta ou destruição, e define dados de saúde como quaisquer informações relacionadas à saúde física ou mental de uma pessoa, abrangendo uma ampla gama de informações como número do SNS, resultados de exames, e históricos clínicos (Lima, 2021).

De seguida, o estudo expõe também os direitos que o RGPD garante aos titulares dos dados, incluindo o direito de acesso, retificação, apagamento, limitação do tratamento, portabilidade dos dados e oposição. Nesse seguimento, Rita Lima alerta para os cuidados a ter na prática diária, como a segurança na visualização de equipamentos e documentos médicos contra terceiros e o uso apropriado das redes sociais pelos profissionais de saúde (Lima, 2021).

Além destes aspetos, abordam-se ainda situações específicas não reguladas pelo regulamento, onde a divulgação de dados pessoais pode ocorrer sem consentimento, como em contextos jornalísticos, artísticos ou académicos. No entanto, a importância da confidencialidade nos casos aplicáveis é reforçada com o aviso de que a sua violação pode resultar em consequências disciplinares, civis e criminais (Lima, 2021).

Por fim, o trabalho abrange a Lei nº 58/2019, que reitera a necessidade de demonstrar a aderência aos princípios de licitude, lealdade, transparência, limitação das finalidades, minimização e exatidão dos dados, bem como de integridade e confidencialidade no tratamento dos mesmos. Sob forma de conclusão, o curso apresenta uma série de exercícios que colocam em prática o conhecimento adquirido, simulando situações reais onde os profissionais de saúde podem ter de aplicar o RGPD, como no trato com familiares de vítimas, agentes policiais ou jornalistas (Lima, 2021).

No âmbito internacional, Eini Koskimies *et al.* realizou um estudo intitulado "*The informational privacy of patients in prehospital emergency care - Integrative literature review*" constituído por uma revisão de literatura que examina a privacidade digital dos pacientes nos cuidados de emergência pré-hospitalar. Utilizando bases de dados como

CINAHL, *MEDLINE* e *Cochrane*, os autores selecionaram onze estudos pertinentes para apreciação, aplicando a técnica de análise de conteúdo para sintetizar as informações (Koskimies *et al.*, 2020).

Os principais resultados do estudo indicam que a privacidade digital é um conceito frequentemente associado à confidencialidade e apresenta várias facetas no contexto da emergência e socorro. A literatura disponível, embora limitada, foca primariamente na privacidade e na confidencialidade, ressaltando a importância do controlo da informação pelas vítimas e da proteção desses dados pelos profissionais de saúde. Foi observado que vários fatores influenciam a garantia da privacidade, incluindo a formação dos próprios técnicos, as práticas de proteção de dados e os desafios únicos inerentes ao ambiente de cuidados pré-hospitalares, como a natureza imprevisível e urgente das situações (Koskimies *et al.*, 2020).

Dado os resultados obtidos, o trabalho destaca a necessidade urgente de mais formação para os socorristas em relação à proteção dos dados sensíveis, sugerindo que uma maior conscientização e educação podem melhorar significativamente a maneira como a privacidade das vítimas é mantida durante os cuidados de emergência. Ademais, o estudo conclui que ainda existe uma grande lacuna na literatura focada especificamente na privacidade em contexto pré-hospitalar, sublinhando a necessidade de pesquisas futuras que abordem este aspeto crucial (Koskimies *et al.*, 2020).

Para além da componente humana, também os sistemas e dispositivos informáticos devem ser analisados na perspetiva da proteção dos dados das vítimas. Nesse sentido, o estudo "*A Comprehensive Literature Review on Privacy, Security, and Data Management in Healthcare*", realizado em 2024 por Singh Y. *et al*, concentra-se nas implicações de segurança e privacidade dos registos eletrónicos de saúde (EHRs). Esta revisão sistemática de literatura aborda os desafios associados à gestão desses registos, destacando as vulnerabilidades e os riscos de violações de privacidade e ciberataques que acompanham a digitalização dos sistemas de saúde (Singh, 2024).

Os autores identificam questões críticas como o acesso não autorizado a dados de saúde, sublinhando a necessidade de mecanismos robustos de segurança para prevenir falhas e manter a confiança das vítimas através da proteção efetiva dos seus dados. As soluções propostas no documento incluem a adoção de princípios de *Privacy by Design*, a implementação de melhores práticas e padrões de segurança e o uso de tecnologias

avançadas, como inteligência artificial e *machine learning*, para análises de dados que não comprometem a privacidade do indivíduo (Singh, 2024).

Finalmente, o documento conclui destacando a necessidade contínua de pesquisa e desenvolvimento de métodos de proteção de dados de saúde, para enfrentar os desafios emergentes na era digital e equilibrar a acessibilidade dos dados com a proteção rigorosa da privacidade dos seus titulares (Singh, 2024).

Através de uma conferência, Mitra A. *et al.* apresentaram um *paper* - "*A Strategic Data Protection Plan for the Healthcare Industry: A Review*" - que explora as estratégias para proteger dados no setor de saúde, enfatizando a necessidade crescente de proteção devido ao aumento significativo da digitalização e da recolha de dados. A pesquisa aborda várias dimensões da proteção de dados, incluindo a implementação de governança de dados eficaz e a adesão a regulamentações de privacidade para evitar a perda de informações confidenciais derivadas de incidentes de segurança (Mitra *et al.*, 2023).

Os autores abordam o impacto das tecnologias emergentes, como a automação robótica de processos e a computação em nuvem, que estão a ampliar os horizontes do setor de saúde, gerando quantidades massivas de dados e, por consequência, aumentando a responsabilidade de protegê-los contra ameaças externas. Nesse sentido, o estudo utiliza uma análise bibliométrica para discutir as atividades de pesquisa recentes sobre a proteção de grandes volumes de dados, destacando a importância de uma estratégia de proteção de dados avançada e padronizada (Mitra *et al.*, 2023).

Por fim, o documento conclui que a análise realizada ilustra a relevância das políticas de privacidade e segurança de dados na saúde, apontando para a urgência de adotar padrões internacionais robustos para melhorar a segurança das informações sensíveis. A pesquisa destaca também a necessidade de investigações contínuas sobre medidas de proteção de dados, especialmente em organizações de saúde, face aos desafios emergentes e à crescente importância dessa temática no contexto global (Mitra *et al.*, 2023).

No norte da Europa, Prosper Yeng, juntamente com os seus colegas coautores, desenvolveu um estudo intitulado "*Framework for Healthcare Security Practice Analysis, Modeling and Incentivization*" que propõe uma análise detalhada das práticas de proteção de dados de saúde, introduzindo um quadro chamado HSPAMI (*Healthcare Security Practice Analysis, Modeling and Incentivization*). Este modelo foi desenhado para alinhar os

procedimentos de segurança dos profissionais de saúde com as regulamentações e padrões internacionais e nacionais, como o RGPD, a ISO 7799 e a legislação norueguesa (Yeng *et al.*, 2019)

Assim, o projeto HSPAMI, financiado pelo Ministério da Saúde e Cuidados da Noruega e operado pelo Centro de Segurança Cibernética e Informação da NTNU, foca em mitigar violações de dados no setor de saúde por meio da identificação de discrepâncias entre as práticas de segurança atualmente adotadas pelos profissionais, como o uso de redes sociais, o armazenamento de documentos sensíveis e a gestão das comunicações via telefónica, e as práticas recomendadas pela regulamentação existente. O estudo salienta que, apesar da importância crítica da tecnologia na proteção de dados, os próprios profissionais de saúde frequentemente representam o elo mais fraco na cadeia de segurança (Yeng *et al.*, 2019).

Como tal, o HSPAMI analisa, em termos práticos, diversos comportamentos de segurança dos funcionários em cenários como *phishing* e engenharia social, usando técnicas qualitativas como observações e entrevistas, além de métodos quantitativos para modelar e analisar as práticas de segurança (Yeng *et al.*, 2019).

Como conclusão dos resultados obtidos, o documento ressalta, à semelhança dos restantes estudos, a necessidade de treinamento e conscientização em segurança como medidas preventivas e corretivas essenciais para reforçar boas práticas de segurança e construir uma forte cultura de segurança entre os profissionais de saúde (Yeng *et al.*, 2019).

Na perspetiva da problemática, os estudos "*Cybersecurity Challenges in Healthcare Systems*", de Singh G. *et al*. (Singh *et al.*, 2024), e "*A Review of Cybersecurity Challenges and Recommendations in the Healthcare Sector*", de Shingari N. *et al*. (Shingari *et al.*, 2023), mergulham nos desafios específicos que o setor de saúde enfrenta em termos de Cibersegurança. Ambos os documentos destacam como a crescente digitalização dos serviços de saúde aumentou a superfície de ataque para cibercriminosos e expôs o setor a novos níveis de vulnerabilidade digital. Além disso, os trabalhos analisam as consequências das violações de dados, ataques de *ransomware*, ameaças internas e os desafios de conformidade regulatória, sublinhando a complexidade de manter a segurança da infraestrutura tecnológica de saúde (Singh *et al.*, 2024), (Shingari *et al.*, 2023).

Ao longo de ambos os estudos, os autores discutem a necessidade de uma cultura de segurança mais robusta dentro das organizações de saúde, enfatizam a importância da

formação contínua em Cibersegurança para todos os níveis de pessoal e aconselham a implementação de políticas de segurança que sejam abrangentes e adaptáveis às rápidas mudanças no panorama de ameaças. Como tal, os trabalhos sugerem a adoção de *frameworks* internacionais de segurança, como o NIST e o ISO, para orientar as práticas de segurança, e recomendam tecnologias emergentes como inteligência artificial e *blockchain* para melhorar a deteção de ameaças e a segurança dos dispositivos médicos conectados (Singh *et al.*, 2024), (Shingari *et al.*, 2023).

Finalmente, as publicações concluem com a recomendação de que políticos, entidades de saúde e profissionais de Cibersegurança colaborem para o desenvolvimento de estruturas de segurança robustas e para a promoção de uma cultura de segurança e resiliência. Sublinham também a necessidade de investimento contínuo em soluções de segurança e vigilância contra ameaças para proteger a integridade dos serviços de saúde e manter a confiança dos titulares dos dados (Singh *et al.*, 2024), (Shingari *et al.*, 2023).

A medicina de emergência e o socorro pré-hospitalar compartilham desafios semelhantes em termos de privacidade e confidencialidade, uma vez que ambos os contextos exigem a gestão cuidadosa de informações sensíveis em ambientes altamente dinâmicos e muitas vezes públicos.

Nesse sentido, o artigo "*Privacy and Confidentiality in Emergency Medicine: Obligations and Challenges*", de Geiderman J. e demais autores, apesar de publicado no ano de 2006, oferece uma análise ainda bastante atual e abrangente das obrigações e desafios associados à privacidade e confidencialidade na medicina de emergência. O documento detalha situações cotidianas em ambientes de urgência onde estes princípios são desafiados, oferecendo estratégias éticas e legais para a sua gestão (Geiderman *et al.*, 2006).

Os autores começam por diferenciar os conceitos de privacidade e confidencialidade, explicando que, embora relacionados, apresentam nuances importantes.

A privacidade aparece descrita como um direito mais amplo que inclui isolamento físico, proteção de informações pessoais, proteção da identidade pessoal e a capacidade de fazer escolhas sem interferência.

Já a confidencialidade foca especificamente na proteção de informações pessoais e, no contexto da saúde, ao dever de não divulgar informações que foram transmitidas ao profissional sem a aprovação do paciente (Geiderman *et al.*, 2006).

A discussão estende-se às bases morais e legais dessas obrigações, incluindo uma revisão da legislação federal e estadual relevante nos Estados Unidos, como o HIPAA (*Health Insurance Portability and Accountability Act*), que impõe regras rigorosas sobre o tratamento de informações de saúde protegidas (Geiderman *et al.*, 2006).

No que toca aos desafios, o artigo aborda também dificuldade práticas, como o *design* de departamentos de emergência para maximizar a privacidade, a gestão de observadores e visitantes, a interação com a aplicação da lei, e as implicações de filmagens comerciais e não comerciais em ambientes de emergência. Para estes obstáculos, os autores propõem soluções práticas para garantir que os direitos dos pacientes à privacidade e confidencialidade sejam mantidos, mesmo em situações de alto stresse e fluxo rápido de trabalho característicos dos serviços de emergência hospitalares e pré-hospitalares (Geiderman *et al.*, 2006).

Finalmente, o artigo sublinha que, apesar dos desafios presentes em ambientes de emergência muitas vezes complexos, é fundamental que os profissionais de saúde mantenham o compromisso de proteger a privacidade e a confidencialidade das vítimas. Estas obrigações, assentes em princípios éticos, legais e filosóficos, são cruciais para respeitar a dignidade e a autonomia das vítimas. Na análise final, verificou-se que poderá ser necessário sobrepor esses deveres em face de obrigações maiores, embora as circunstâncias que justifiquem essa invasão sejam extremamente raras (Geiderman *et al.*, 2006).

Ainda na dimensão internacional, também o artigo "*From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine—Part II: Challenges in the Emergency Department*", escrito no estado de Carolina do Norte (USA) por John Moskop e coautores, foca em questões específicas de confidencialidade enfrentadas nos departamentos de emergência. O estudo destaca problemas relacionados à privacidade física, como o *design* das infraestruturas de urgência que muitas vezes não oferece salas individuais, resultando na prestação de cuidados em grandes áreas com divisórias simples, como cortinas (Moskop *et al.*, 2005). No contexto da emergência pré-hospitalar, que ocorre diversas vezes em locais públicos, tal como em ruas ou espaços abertos, também esta privacidade física enfrenta desafios similares aos identificados em salas de urgência. Em ambientes externos, a falta de barreiras físicas leva a que as vítimas sejam frequentemente tratadas à vista de terceiros, comprometendo tanto a privacidade física quanto a confidencialidade das suas informações.

Além disso, o artigo aborda o impacto do elevado número de pacientes e a consequente dificuldade em manter a privacidade e a confidencialidade sob essas condições,

mencionando exemplos como a presença de visitantes, polícias, estudantes e outros observadores que podem necessitar de acesso aos utentes por diversas razões. A presença de câmaras e a gravação de atividades também são discutidas, especialmente em contextos de programas de televisão baseados na realidade, que levantam preocupações adicionais sobre a violação da privacidade das vítimas (Moskop *et al.*, 2005).

No que diz respeito às questões de confidencialidade, o estudo examina a proteção dos registos médicos, o dever de alerta sobre situações reportáveis, inquéritos telefónicos de familiares e amigos, e requisições dos média por informações dos pacientes. O artigo também destaca a necessidade de comunicação apropriada entre os profissionais de saúde para assegurar que a informação de cada utente seja partilhada de maneira segura e apenas quando necessário para o tratamento (Moskop *et al.*, 2005).

Finalmente, o trabalho conclui que, apesar dos desafios substanciais, é fundamental que os profissionais de emergência compreendam e cumpram as suas obrigações de proteger a privacidade e a confidencialidade das vítimas, baseando-se em fundamentos morais e legais. As políticas e práticas nos departamentos de emergência devem refletir essa responsabilidade, mesmo em ambientes onde esses valores são difíceis de manter (Moskop *et al.*, 2005).

Foi também na base de dados bibliográfica *ScienceDirect* que Hasan Erbay viu publicado no Jornal Turco de Medicina de Emergência o seu artigo "*Some Ethical Issues in Prehospital Emergency Medicine*", cujo tema remete para as questões éticas enfrentadas no âmbito dos cuidados pré-hospitalares (Erbay, 2014).

Numa abordagem inicial, o documento destaca a complexidade desses aspetos éticos, classificando-os em quatro grupos: o processo antes das intervenções de socorro, incluindo justiça, estigmatização, situações perigosas e direção segura; o processo de tratamento, incluindo triagem, recusa de tratamento ou transporte e consentimento informado; o fim da vida e dos cuidados, incluindo tratamentos de suporte de vida, continuação ou suspensão de manobras de reanimação e presença da família durante o socorro; e alguns problemas de perceção sobre o uso das ambulâncias, incluindo a utilização indevida da ambulância, cuidado de menores e comunicação de más notícias (Erbay, 2014).

É no processo de tratamento que o autor aborda com detalhe a confidencialidade e privacidade da vítima, ressaltando os desafios inerentes à natureza dos ambientes em que

ocorrem as emergências pré-hospitalares, sejam eles residenciais ou laborais. A necessidade de proteger informações de saúde, condições físicas, dados pessoais e detalhes do estilo de vida do paciente é enfatizada, juntamente com a observação de que tais considerações éticas se estendem até após a morte do indivíduo (Erbay, 2014).

Dada a variação na perceção da privacidade de pessoa para pessoa, cada profissional da área encontra frequentemente conflitos éticos ao tentar equilibrar a urgência médica com a manutenção da dignidade e confidencialidade da vítima. Estes dilemas não só desafiam os protocolos de socorro como também requerem uma abordagem sensível e adaptada a cada situação específica, garantindo que os direitos e desejos dos titulares dos dados sejam respeitados mesmo em circunstâncias de crise (Erbay, 2014).

O estudo conclui que os cenários de emergência pré-hospitalar apresentam desafios significativamente maiores para os profissionais de saúde do que o ambiente controlado das salas de emergência hospitalar. No local das ocorrências, cada vítima e situação são únicas, com implicações éticas também distintas para cada caso (Erbay, 2014).

Assim, o autor considera que não existem soluções rápidas ou fórmulas prontas para ações e decisões corretas. Torna-se, portanto, crucial que os profissionais tenham conhecimento ético e legal suficiente para tomar as melhores decisões *a priori* em casos complexos. Além disso, dada a singularidade e a complexidade das questões éticas nesta área, considera-se fundamental estabelecer protocolos que enfrentem esses desafios de maneira eficaz (Erbay, 2014).

Além de garantir a proteção dos dados, é também fundamental assegurar o acesso adequado a essas informações, de forma a otimizar a prestação de cuidados de saúde em situações de emergência.

Nesse sentido, o estudo "*Are prehospital treatment or conveyance decisions affected by an ambulance crew's ability to access a patient's health information?*", conduzido por Ollie Zorab e coautores, explora a influência do acesso à informação de saúde das vítimas nas decisões de tratamento ou transporte por equipas de ambulância. À semelhança dos objetivos para o presente estudo, esta pesquisa envolveu também um inquérito online com operacionais de um serviço regional de ambulâncias no Reino Unido, centrando-se na experiência deles ao acederem à informação de saúde das vítimas e como isso afetou a tomada de decisões clínicas (Zorab *et al.*, 2015).

Os resultados indicaram que a maioria dos profissionais enfrentava dificuldades significativas ao aceder à informação de saúde dos pacientes, e acreditava que um melhor acesso poderia conduzir a uma seleção mais apropriada de vias de cuidado. A falta de acesso a informações cruciais como histórico médico, ordem de não reanimação ou desejos de cuidados no final da vida foi frequentemente apontada como um obstáculo que poderia levar à escolha desadequada de procedimentos de socorro (Zorab *et al.*, 2015).

O estudo conclui que as decisões sobre os cuidados mais apropriados para as vítimas atendidas pelos serviços de emergência são melhor informadas quando existe acesso a informações de saúde precisas e completas. Dessa forma, sugere-se a necessidade urgente de sistemas melhorados que permitam o acesso em tempo real às informações de saúde da vítima, a fim de apoiar as decisões clínicas em ambientes pré-hospitalares. A pesquisa termina realçando a importância da integração e comunicação entre diferentes serviços de saúde para otimizar os resultados dos pacientes e reduzir encaminhamentos desnecessários para serviços de urgência (Zorab *et al.*, 2015).

Ainda dentro do contexto pré-hospitalar, também o estudo "*Paramedics' Perspectives on Patient's Informational Privacy in Prehospital Emergency Care*", de Eini Koskimies *et al*, investiga a privacidade das informações das vítimas no contexto da emergência e socorro pré-hospitalar da Finlândia. O foco central do estudo assenta na perceção de como essa privacidade é percebida e realizada pelos paramédicos, juntamente com os fatores que influenciam a sua efetivação. A pesquisa empregou um desenho de estudo descritivo, utilizando um questionário para recolher dados de 26 paramédicos de um dos 22 departamentos de resgate na Finlândia, com a aprovação do comité de ética da Universidade de Turku (Finlândia) (Koskimies *et al.*, 2019).

Os resultados do estudo indicam que os profissionais percebem a privacidade da vítima principalmente como o direito da mesma à confidencialidade das suas informações de saúde e a um respeito geral pela proteção desses dados por parte dos intervenientes no socorro. Apesar da privacidade destas informações ser geralmente bem salvaguardada em termos de elaboração de relatórios e gestão dos registos de saúde, notou-se que a eficácia dessa proteção pode variar de acordo com o contexto (Koskimies *et al.*, 2019).

Identificaram-se também fatores que tanto promovem como prejudicam a proteção efetiva da privacidade dos dados. Entre os facilitadores, destacam-se a competência profissional dos paramédicos, o ambiente laboral, a formação recebida e as diretrizes

seguidas. Por outro lado, a natureza exigente do trabalho, as atitudes dos próprios socorristas e o desconhecimento sobre a importância da privacidade dos dados entre os profissionais, as entidades colaboradoras, as vítimas e os familiares foram apontados como obstáculos (Koskimies *et al.*, 2019).

O estudo conclui que, apesar de existir uma compreensão abrangente sobre a privacidade da informação e os fatores que influenciam a sua proteção entre os paramédicos, ainda se verifica uma variação na sua implementação eficaz. Assim, de acordo com a opinião dos autores, é necessário desenvolver mais investigações e formação nesta área para melhorar a proteção dos dados sensíveis envolvidos e assegurar um atendimento de emergência pré-hospitalar equitativo e de alta qualidade para toda a sociedade (Koskimies *et al.*, 2019).

2.2. Conclusões

Numa perspetiva geral, o panorama do tratamento e proteção de dados no setor da saúde tem vindo a ser amplamente explorado ao longo dos últimos anos. No entanto, observa-se ainda uma limitação em relação à existência de literatura específica no contexto de socorro pré-hospitalar (Koskimies *et al.*, 2020). Uma grande parte dos documentos existentes concentra-se em ambientes hospitalares e em sistemas de saúde já estruturados, enquanto o contexto de emergência médica recebe atenção limitada, apesar da sua relevância na recolha e tratamento de informações sensíveis em situações urgentes.

Adicionalmente, verifica-se que uma grande parte da literatura analisada está centrada exclusivamente no impacto e nas exigências do RGPD. Compreende-se que tal facto esteja associado ao amplo reconhecimento deste regulamento como um marco transformador na proteção de dados, impondo relevantes normas e responsabilidades às organizações de saúde da União Europeia.

No entanto, existem desafios específicos no contexto do socorro pré-hospitalar que podem limitar a eficácia deste regulamento. Primeiramente, a sua natureza ampla não aborda particularidades emergentes nas situações de emergência, onde decisões rápidas sobre o tratamento de dados de saúde são cruciais. Além disso, a obtenção de consentimento explícito, uma exigência central do RGPD para o tratamento de dados sensíveis, pode ser impraticável no momento da ocorrência, criando barreiras legais que podem impedir o socorro. Por último, as estritas normas do regulamento sobre a transferência de dados podem

complicar a necessária comunicação rápida entre os diversos intervenientes no socorro. Tais desafios destacam a necessidade de uma análise atenta da legislação, focando nas especificidades do socorro pré-hospitalar.

Apesar de tudo isto, os estudos existentes convergem em algumas áreas fundamentais ao desenvolvimento do presente estudo, tais como:

1. **Relevância do RGPD**: O RGPD é unanimemente considerado a principal referência normativa para a proteção de dados na saúde, visto que reforça os direitos dos titulares, como o acesso, a portabilidade, o apagamento e a oposição, além de introduzir princípios inovadores como "*privacy by design*" e "*privacy by default*";

2. **Confidencialidade e sigilo profissional**: A proteção de dados é vista como uma extensão dos princípios éticos tradicionais, como o sigilo profissional. Os estudos destacam a necessidade de garantir que informações sensíveis sejam tratadas exclusivamente para as finalidades previstas, protegendo a privacidade do titular em todas as etapas do processo de cuidados;

3. **Desafios na implementação**: A adaptação à legislação é apontada como um desafio comum, especialmente devido à insuficiência de recursos humanos, tecnológicos e financeiros nas organizações de saúde. Muitas vezes, as iniciativas limitam-se a ações básicas, como a identificação de bases de dados e treinamentos pontuais, sem atingir um nível estratégico;

4. **Tecnologia e riscos**: O avanço da digitalização na saúde, incluindo a utilização de sistemas como o Registo de Saúde Eletrónico (RSE) e *Big Data*, é reconhecido como uma oportunidade para melhorar os cuidados. No entanto, também é uma fonte de vulnerabilidades, como acessos não autorizados e falhas na segurança;

5. **Necessidade de governança estruturada**: A nomeação de Encarregados de Proteção de Dados (DPOs), a realização de avaliações de impacto e a criação de políticas claras de tratamento de dados são práticas recomendadas e destacadas em quase todos os trabalhos;

6. **Lacunas no conhecimento**: Existe um consenso sobre a falta de formação adequada para profissionais de saúde em geral. Essa deficiência prejudica a compreensão e aplicação das normas existentes, aumentando o risco de não conformidade e sanções.

Em resumo, embora exista uma base sólida de literatura sobre proteção de dados na saúde, esta é quase inteiramente direcionada ao RGPD e aos ambientes hospitalares. As lacunas em contextos específicos, como o pré-hospitalar, e os desafios práticos de implementação evidenciam a necessidade de esforços adicionais para promover uma proteção de dados mais ampla e eficaz.

3. Emergência pré-hospitalar

Para enquadrar a legislação de tratamento e proteção de dados no contexto da emergência pré-hospitalar, torna-se essencial compreender primeiro a definição e funcionamento desta área e os serviços de socorro que operam em Portugal.

De forma a melhor compreender o tema em questão, sugere-se, numa primeira abordagem, a compreensão separada de ambas as palavras que caracterizam esta atividade profissional. Assim, uma emergência (médica) entende-se por qualquer situação súbita e inesperada que representa um risco imediato à vida ou à saúde de uma pessoa, exigindo intervenção médica rápida para prevenir agravamentos ou mortes (INEM, 2020). Já o conceito de pré-hospitalar remete ao conjunto de intervenções e cuidados médicos prestados fora do ambiente hospitalar, geralmente no local de ocorrência da emergência, com o objetivo de estabilizar a vítima até que esta possa ser transportada para unidade hospitalar (Marra, 2023).

Com uma média nacional diária de 4149 chamadas de emergência realizadas em 2023 ao CODU do INEM (INEM, 2024), torna-se clara a necessidade de existência de uma estrutura organizada e de uma rede de serviços robusta, onde o tempo de resposta é crucial. Nesse sentido, ao longo de várias décadas, o panorama da emergência pré-hospitalar em Portugal evoluiu significativamente, buscando adaptar-se às crescentes exigências de eficácia e prontidão no atendimento.

Uma vez que a capacidade de agir rapidamente pode fazer a diferença entre a vida e a morte, começou a ser necessário por parte das equipas de socorro o acesso imediato a informações relevantes sobre o estado de saúde das vítimas, incluindo, por exemplo, histórico médico, alergias e outras condições que possam influenciar a ocorrência.

Para dar resposta a esta necessidade, nos últimos anos as estratégias de socorro foram também reforçadas com o desenvolvimento tecnológico, através da integração de sistemas de comunicação em rede, GPS para localização rápida e sistemas eletrónicos de registo, que auxiliam na recolha e troca de dados entre as equipas no terreno e as unidades hospitalares. No entanto, apesar da importância destas ferramentas para o atendimento, muitas áreas ainda recorrem a suportes físicos, como formulários de papel, especialmente em situações onde os meios digitais não estão acessíveis. Esses dados recolhidos e compartilhados são críticos

para a eficácia das operações, mas também geram uma responsabilidade adicional para os profissionais, que devem assegurar que as informações sejam tratadas de forma confidencial e em conformidade com as normas de proteção de dados.

Assim, neste capítulo, explora-se a evolução histórica, o sistema que estrutura o socorro a nível nacional, os recursos tradicionais e tecnológicos que apoiam cada ocorrência, bem como os tipos de dados recolhidos e as várias situações em que essas informações se tornam indispensáveis. Esta contextualização é essencial para uma posterior análise mais detalhada das implicações legais e éticas no tratamento de dados em situações de emergência.

3.1. Evolução histórica

A evolução da emergência pré-hospitalar em Portugal reflete o trabalho conjunto de diversas entidades que contribuíram para estabelecer um sistema de socorro eficaz e coordenado ao longo de décadas.

Os primeiros serviços de socorro de âmbito pré-hospitalar remontam à década de sessenta, com a introdução do número nacional de emergência (à época, 115), ativando ambulâncias tripuladas por polícias para transportar doentes para o hospital mais próximo, em Lisboa (Leitão, 2022).

Após isso, no início da década de setenta, foi criado o Serviço Nacional de Ambulâncias, composto por meios medicalizados entregues à PSP e às corporações de Bombeiros existentes, que centralizou a gestão das atividades de primeiros socorros e transporte de doentes e estabeleceu as bases para o desenvolvimento de um posterior Sistema Integrado de Emergência Médica (SIEM) (Leitão, 2022). Assim, este sistema veio reunir um conjunto de entidades que interagiam com um propósito comum: prestar assistência às vítimas de doença súbita ou acidente. Desse conjunto fazem atualmente parte a PSP, a GNR, o INEM, os Bombeiros, a Cruz Vermelha Portuguesa, os Centros Hospitalares e os Centros de Saúde (INEM, s.d.).

Já a 3 de agosto de 1981 foi fundado o Instituto Nacional de Emergência Médica (INEM), consolidando a coordenação das atividades de emergência médica. Nessa altura, esta entidade organizou formações para equipas médicas, bombeiros e polícias, e criou o Centro de Orientação de Doentes Urgentes em 1987, que possibilitou a triagem telefónica e o acionamento de meios de socorro, 24 horas por dia. Com a introdução das primeiras

Viaturas Médicas de Intervenção Rápida (VMIR) e, posteriormente, das Viaturas Médicas de Emergência e Reanimação (VMER), o INEM expandiu a sua capacidade de resposta, implementando novas tecnologias e aumentando a cobertura dos serviços (Leitão, 2022).

Ainda que o INEM, organismo atualmente sob responsabilidade do Ministério da Saúde, possua aos dias de hoje uma vasta diversidade de meios especializados, foram as Associações de Bombeiros Voluntários que desempenharam um papel crucial na emergência pré-hospitalar em localidades onde o Instituto ainda não possuía infraestruturas próprias (INEM, 2021). Assim, as associações humanitárias, presentes em todo o país, foram historicamente responsáveis pelo transporte de doentes e pela prestação de primeiros socorros além das grandes cidades, muitas vezes de forma voluntária e com recursos limitados (INEM, 2021). A Cruz Vermelha, por sua vez, complementou as operações de emergência ao oferecer apoio em situações de crise, numa primeira instância socorrendo feridos e doentes militares em tempo de guerra, e mais tarde provendo ambulâncias e socorristas para também responder a emergências envolvendo civis (CVP, s.d.).

Nos últimos anos, com o apoio dos avanços tecnológicos e do aumento do investimento em formação especializada, as entidades de emergência pré-hospitalar em Portugal, incluindo INEM, Bombeiros e Cruz Vermelha, conseguiram coordenar os seus esforços de forma mais integrada. Esta colaboração ampliou a cobertura dos serviços, reduziu os tempos de resposta e melhorou a qualidade dos cuidados prestados, assegurando que a população tenha acesso a uma assistência rápida e eficiente em situações de emergência.

Por outro lado, toda esta evolução veio enfatizar a quantidade e diversidade de dados que foram sendo e continuam a ser armazenados e geridos por todas estas entidades ao longo de dezenas de anos, evidenciando a necessidade de implementação de políticas robustas para proteção e gestão de toda essa informação.

3.2. Sistema Integrado de Emergência Médica

Tal como abordado anteriormente, a 11 de Março de 1980, a Resolução nº 84 do Conselho de Ministros criou o Gabinete de Emergência Médica (GEM) que teve como principal objetivo o desenvolvimento e a coordenação de um Sistema Integrado de Emergência Médica (SIEM) (INEM, 2013). Com vista à implementação desse sistema, o INEM estabeleceu durante os anos seguintes à sua fundação diversas bases de colaboração com as entidades que, aos dias de hoje, possuem responsabilidades de socorro (INEM, 2013).

Assim, o SIEM caracteriza-se atualmente como um conjunto de ações coordenadas, de âmbito pré-hospitalar, hospitalar e inter-hospitalar, que resultam da intervenção ativa e dinâmica dos vários componentes do sistema nacional de saúde. Este modelo permite uma atuação rápida, eficaz e económica em situações de emergência médica, englobando o socorro pré-hospitalar, o transporte, a receção hospitalar e a referência adequada do doente urgente/emergente (INEM *et al.*, 2024).

A "Estrela da Vida" é o símbolo internacional dos serviços de emergência médica. É composta por seis faixas, tendo localizado no seu centro, ao alto, o bastão de Esculápio com uma serpente enrolada. As seis faixas correspondem às fases que constituem um ciclo completo de ações em termos de Emergência Médica (INEM *et al.*, 2024).

Nesse sentido, cada uma das pontas da estrela corresponde a uma das diferentes fases do SIEM (INEM *et al.*, 2024).

- **Deteção:** Momento de perceção da existência de uma ou mais vítimas de doença súbita ou acidente;
- **Alerta:** Fase de contacto com os serviços de emergência, através do Número Europeu de Emergência – 112;
- **Pré-socorro:** Conjunto de gestos simples que podem e devem ser efetuados até à chegada do socorro;
- **Socorro:** Cuidados de emergência iniciais efetuados às vítimas, com o objetivo de as estabilizar, diminuindo assim a morbilidade e a mortalidade;
- **Cuidados durante o transporte:** Transporte assistido da vítima numa ambulância com características, tripulação e carga bem definidas, desde o local da ocorrência até à unidade de saúde adequada, garantindo a continuação dos cuidados necessários;
- **Transferência e tratamento definitivo:** Tratamento no serviço de saúde mais adequado ao estado clínico da vítima. Em alguns casos excecionais, pode ser necessária a intervenção inicial de um estabelecimento de saúde onde são prestados cuidados imprescindíveis para a estabilização da vítima, com o objetivo de garantir um transporte mais seguro para um hospital mais diferenciado e/ou mais adequado à situação.

Todas estas etapas de resposta em emergência enfatizam a complexidade e a interdependência dos vários intervenientes envolvidos na ocorrência. Cada fase exige ações específicas e coordenadas, que só podem ser realizadas de forma eficaz se houver acesso

rápido e preciso a dados pessoais e clínicos das vítimas. Este fluxo de informações entre os serviços de emergência é fundamental para garantir a continuidade e qualidade dos cuidados. Assim, a necessidade de acesso a esses dados ao longo das fases do SIEM realça também a importância de assegurar a proteção e confidencialidade das informações, respeitando a privacidade das vítimas e cumprindo as regulamentações legais existentes.

3.2.1. Entidades e profissionais intervenientes

Criado em 1991, o número de emergência nos países da UE é o conhecido 112. Não precisa de indicativo, é gratuito e pode ser marcado a partir de dispositivos das redes fixa (incluindo telefones públicos) ou móvel, tendo prioridade sobre as outras chamadas (INEM *et al.*, 2024).

Em Portugal, as chamadas realizadas para o Número Europeu de Emergência são atendidas em quatro centros operacionais: dois no continente (norte e sul), um na Região Autónoma da Madeira (COMDR) e outro na Região Autónoma dos Açores (COAZR), estando estes últimos interligados com o território continental, garantindo assim capacidades alternativas e de redundância entre todos os centros operacionais. A estes centros, sob responsabilidade da Direção Nacional da Polícia de Segurança Pública, compete o atendimento ao público, a identificação e caracterização das ocorrências, o apoio especializado em situações especiais e, principalmente, o reencaminhamento das situações de emergência para as entidades competentes (INEM *et al.*, 2024).

Apesar de representarem o primeiro contacto direto com a ocorrência, são poucas as situações em que os centros operacionais necessitam de previamente solicitar e recolher dados das vítimas de emergências médicas. Tal facto deve-se, numa primeira instância, à ausência de necessidade de recolha antecipada de informações detalhadas das vítimas, já que os CODU realizam novamente essa recolha no momento em que ativam o socorro. Ao garantir que todas as informações relevantes são obtidas diretamente dos próprios serviços de emergência médica, reduz-se a redundância na recolha de dados e evita-se o risco de informações desatualizadas ou incorretas.

Além disso, a proteção de dados é outro fator relevante. Uma vez que as forças de segurança não necessitam de manter dados pessoais ou clínicos das vítimas no seu sistema, evita-se o armazenamento e a manipulação de informações sensíveis por entidades que não têm uma função clínica direta. Esta prática respeita princípios básicos de proteção de dados, amplamente abordados nas regulamentações que virão a ser exploradas neste estudo,

garantindo que apenas os serviços responsáveis pela assistência médica tenham acesso às informações estritamente necessárias para o atendimento.

Atualmente, a nível continental, as chamadas que dizem respeito a situações de saúde são encaminhadas para os Centro de Orientação de Doentes Urgentes do INEM em funcionamento no Porto, Coimbra, Lisboa e Faro (INEM *et al.*, 2024).

Ao CODU compete atender e avaliar no mais curto espaço de tempo os pedidos de socorro recebidos, com o objetivo de determinar os recursos necessários e adequados a cada situação. O funcionamento do CODU é assegurado em permanência por Médicos, Técnicos de Emergência Pré-Hospitalar e Psicólogos. Todos estes profissionais possuem formação específica para, essencialmente, avaliar a situação do outro lado da linha com o objetivo de determinar recursos necessários e adequados a cada caso, selecionar e acionar os meios de socorro, e ainda assegurar o contacto com as unidades de saúde, transmitindo alguns dados obtidos no terreno de forma a preparar a receção hospitalar (INEM *et al.*, 2024).

Durante a realização dessas tarefas, os elementos que trabalham nestes centros lidam com diversos dados relativos às vítimas e à situação em que estas se encontram, informações essas essenciais para uma triagem eficaz, permitindo aos profissionais do CODU a tomada de decisões rápidas e bem-informadas sobre os recursos e meios a mobilizar. Contudo, o manuseio e processamento de tais informações sensíveis exige cuidados redobrados para garantir a confidencialidade e a segurança dos dados, assegurando que as informações partilhadas entre o CODU, os meios de socorro e as unidades de saúde sejam limitadas ao necessário.

Além das infraestruturas e dos profissionais envolvidos no atendimento de primeira linha, para que o SIEM possa prestar uma assistência pré-hospitalar efetiva à vítima, é também essencial a existência de meios de socorro adequados para cada situação.

Atualmente, o INEM dispõe de uma ampla diversidade de veículos de socorro e apoio às ocorrências. Prova disso são os indicadores de desempenho apresentados pela entidade, conforme ilustrado na Figura 2, que revelam um total de 714 meios de emergência pré-hospitalar em operação ao serviço da sociedade em 2024 (INEM, 2024).

Assim, a análise dos dados estatísticos apresentados pela mesma Figura permitem observar a quantidade de meios disponíveis por categoria, incluindo helicópteros, VMERs, TIPs, SIVs, AEMs, MEMs, UMIPEs, ASs, entre outros (INEM, 2024).

Da totalidade destes meios, destacam-se as duas tipologias de ambulâncias de socorro, com 445 e 94 veículos, respetivamente (Figura 2). A maior parte das Corporações de Bombeiros estabeleceu com o INEM protocolos para se constituírem como Posto de Emergência Médica ou Posto Reserva. Muitas das delegações da CVP são postos reserva do INEM. As ambulâncias PEM são ambulâncias de socorro do INEM, que estão sediadas em corpos de Bombeiros com os quais a entidade de saúde celebrou protocolos. Estas ambulâncias destinam-se à estabilização e transporte de doentes que necessitem de assistência durante o transporte e cuja tripulação e equipamento permitem a aplicação de medidas de suporte básico de vida (SBV) e desfibrilhação automática externa (DAE). A tripulação é constituída por dois elementos da corporação e, pelo menos um deles, deve estar habilitado com o Curso de Tripulante de Ambulância de Socorro (TAS). O outro tripulante, no mínimo, deve estar habilitado com o Curso de Tripulante de Ambulância de Transporte (TAT) (INEM, 2013).

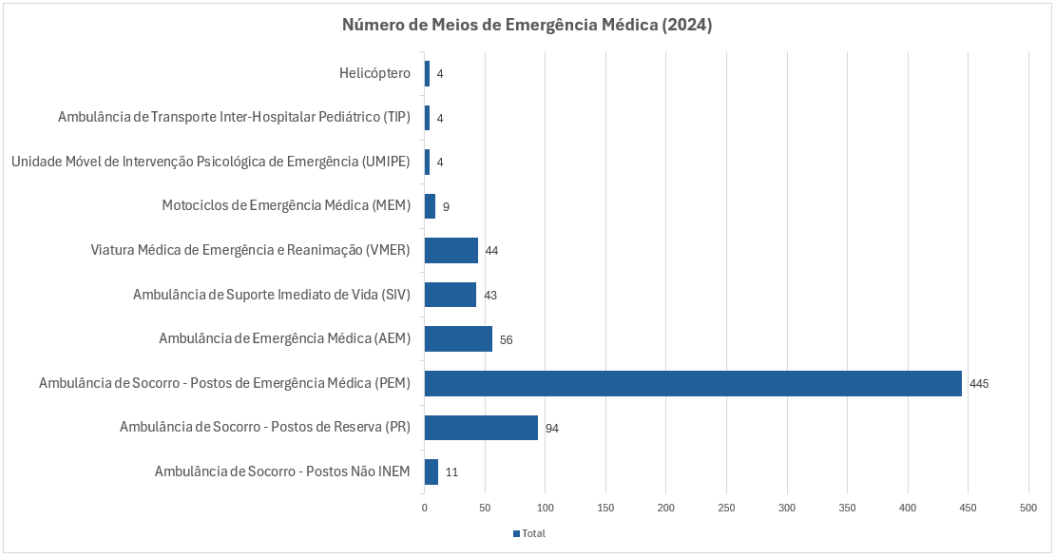


Figura 2 – Número de meios de emergência pré-hospitalar do INEM (adaptado de (INEM, 2024))

Segundo a análise dos meios existentes, as associações de Bombeiros representam cerca de 62% do socorro de emergência pré-hospitalar em Portugal, ficando 13% no âmbito da Cruz Vermelha Portuguesa e os restantes 25% no INEM (INEM, 2024). No entanto, ao excluir deste cálculo todos os veículos do INEM que possuem uma baixa casuística, devido ao facto de estarem destinados a ocorrências mais específicas, a atuação em ocorrências médicas "habituais" cabe em cerca de 80% aos corpos de Bombeiros.

Os profissionais de segunda linha, por serem aqueles que mais tempo prestam em contacto direto com as vítimas, enfrentam uma grande responsabilidade devido à quantidade

de informações sensíveis recolhidas e geradas durante os procedimentos e protocolos de socorro. Esta realidade reforçou a necessidade urgente de criação de formação que viesse capacitar esses trabalhadores quanto ao tratamento e proteção de dados. Como tal, de forma a consciencializar os socorristas assalariados associados às ambulâncias de socorro do INEM, esta entidade promoveu, no ano de 2021, uma ação de formação online, gratuita e obrigatória com o objetivo de fornecer conhecimentos sobre o RGPD aos profissionais que se encontravam formados com o curso de TAS até à data (INEM, 2021).

Ainda nesse mesmo ano, a Escola Nacional de Bombeiros promoveu um *webinar* que visou divulgar junto dos Bombeiros Voluntários a regulamentação existente e os cuidados a observar no que respeita à proteção de dados das vítimas, sempre que intervêm em qualquer tipo de emergência pré-hospitalar (ENB, 2021).

Além disso, para os futuros formandos, o INEM incluiu, recentemente, no novo manual de formação TAS uma secção destinada à proteção de dados das vítimas, demonstrando uma preocupação contínua com o cumprimento da legislação em vigor (INEM *et al.*, 2024).

No entanto, conforme mencionado anteriormente, as ambulâncias de socorro em postos PEM ou PER podem incluir na sua tripulação, no máximo, um elemento da corporação humanitária habilitado com o Curso de TAT (INEM, 2013). Considerando que a formação inicial e atual de um bombeiro voluntário prevê apenas a obrigatoriedade de aprovação neste curso, verifica-se que, na maioria das corporações, apenas uma pequena percentagem dos elementos do quadro ativo possui o Curso de TAS, embora esta realidade tenha vindo a melhorar nos últimos anos.

Nesse contexto, é importante destacar que os elementos habilitados com o curso de TAT, ministrado pelo INEM, ainda não são obrigados, por esta ou qualquer outra entidade, a frequentar e concluir o curso sobre o RGPD anteriormente mencionado. Adicionalmente, até à data de publicação deste estudo, o manual do curso de TAT permanece sem atualizações, sendo a sua última edição datada de 2012 (Valente *et al.*, 2012). Este facto evidencia a necessidade de continuação da reformulação e atualização dos conteúdos formativos, de modo a incluir temas relacionados com a proteção de dados pessoais e clínicos, alinhados com as atuais exigências legais.

Além dos operadores das centrais operacionais e dos socorristas, também todo o pessoal inter-hospitalar desempenha um papel crucial no funcionamento do Sistema Integrado de

Emergência Médica, sendo responsáveis pela receção e tratamento das vítimas após o transporte às unidades de saúde. Estes profissionais são a última etapa do processo de emergência pré-hospitalar, garantindo a continuidade dos cuidados iniciados no terreno.

No momento da chegada à unidade de saúde, a equipa desse turno, composta por médicos, enfermeiros e outros auxiliares e técnicos especializados, deve estar preparada para receber informações detalhadas sobre o estado clínico da vítima, recolhidas e transmitidas previamente pelos serviços de emergência. Esse fluxo de dados, muitas vezes vital para a estabilização ou tratamento definitivo do paciente, exige uma comunicação clara e segura entre os diferentes intervenientes do SIEM. Além disso, é também responsabilidade dos hospitais e centros de saúde assegurar que os dados pessoais e clínicos recebidos sejam tratados de forma confidencial, em conformidade com as normas legais e éticas de tratamento e proteção de dados.

Em resumo, os principais intervenientes no SIEM incluem o cidadão, os operadores das centrais de emergência 112, os agentes da autoridade, os Bombeiros, a Cruz Vermelha Portuguesa, os tripulantes de ambulância, os técnicos de emergência pré-hospitalar, os médicos, os enfermeiros, os auxiliares de saúde, bem como os técnicos de telecomunicações e de informática. Além disso, conclui-se que todos estes profissionais, em diferentes fases do processo de emergência médica, têm acesso a dados pessoais e, frequentemente, a dados clínicos das vítimas. Esse acesso é indispensável para a realização de funções específicas e eficazes, mas exige uma gestão rigorosa, ética e em conformidade com as regulamentações que serão mais à frente exploradas neste estudo.

3.2.2. Fluxo da chamada de emergência

Após identificar as entidades, os profissionais e as infraestruturas envolvidas no socorro, torna-se mais fácil compreender o percurso que os dados seguem ao longo de todo o socorro à vítima. Este fluxo de informações é iniciado no momento em que o cidadão entra em contacto com os centros operacionais 112, operados pelas forças de segurança. Nesta etapa inicial, o operador irá validar a chamada relativamente à sua veracidade e utilidade no contexto da emergência, e sendo-o, procede à sua localização, validando aquela que lhe é apresentada automaticamente por um sistema de suporte ao atendimento (Martins, 2017). Além disso, são também recolhidos dados básicos, como o tipo de emergência e o número estimado de vítimas, que são posteriormente transmitidos às entidades com competência para o socorro da situação em concreto (Martins, 2017).

As únicas exceções a este processo, são as situações de emergência médica, onde, devido à complexidade da sua triagem e processo de decisão, a chamada de voz inicial é, efetivamente, transferida para um dos CODUs do INEM, sem prejuízo de serem também a este disponibilizados todos os dados já anteriormente recolhidos (Martins, 2017).

Após a chamada ser transferida, a situação é analisada por médicos ou técnicos, que avaliam a emergência com maior detalhe, recolhendo informações mais específicas sobre o estado de saúde das vítimas. Durante e após o atendimento, os dados são partilhados com os operadores das centrais de Bombeiros, ou diretamente com as equipas de socorro, recorrendo a uma lista de contactos conhecida e partilhada internamente.

Por fim, a chamada culmina com o armazenamento de todos os dados recolhidos ao longo do atendimento num episódio clínico, que é associado ao historial da vítima. Este registo centralizado permite não apenas documentar a intervenção para fins operacionais e estatísticos, mas também garantir a continuidade dos cuidados, caso sejam necessários tratamentos ou esclarecimentos adicionais em unidades de saúde. Este processo reforça a importância de uma gestão rigorosa dos dados, assegurando que estão devidamente protegidos e acessíveis apenas a profissionais autorizados, em conformidade com as normas legais e éticas aplicáveis.

3.3. Ferramentas e os dados que registam

No contexto da emergência pré-hospitalar, as ferramentas de trabalho desempenham um papel fundamental em todas as etapas do socorro, desde a receção da chamada até ao encerramento da ocorrência. Estes meios incluem tanto sistemas informáticos avançados, que facilitam a gestão e a partilha de dados em tempo real, como os tradicionais registos em papel, ainda amplamente utilizados em diversas fases do processo. Cada um destes instrumentos tem funções específicas, permitindo que os intervenientes recolham, processem e transmitam informações críticas de forma segura e organizada. Este subcapítulo explora as funções e a relevância de ambos os recursos em cada etapa do fluxo de emergência.

3.3.1. Meios tecnológicos

Nas últimas décadas, a tecnologia tem assumido um papel cada vez mais central no sistema de emergência pré-hospitalar, substituindo gradualmente os meios tradicionais em muitas etapas do processo. Ferramentas digitais e sistemas informatizados passaram a

dominar a gestão das ocorrências, permitindo uma comunicação mais rápida, uma coordenação mais eficaz dos recursos e uma maior segurança na partilha de dados. Como tal, atualmente, a digitalização do processo de socorro ocorre em praticamente todas as entidades envolvidas, desde os centros operacionais que recebem as chamadas de emergência, até às equipas de socorro e às unidades hospitalares que recebem as vítimas.

O atendimento de chamadas de emergência é um processo complexo, visto que o cidadão, muitas vezes em estado emocional alterado devido à situação de urgência que vive ou presencia, pode não estar nas condições ideais para fornecer as informações solicitadas pelos agentes e militares dos centros operacionais. Ao mesmo tempo, dado o potencial de cada chamada envolver uma situação crítica, exige-se ao operador uma grande agilidade para estruturar a informação de forma eficiente e sistemática, garantindo que os recursos mais adequados sejam enviados com a maior brevidade possível para uma intervenção precisa (Martins, 2017).

Para que tal possa acontecer de forma eficaz, o operador tem à sua disposição um sistema de suporte ao atendimento, flexível e intuitivo, que lhe permite recolher a informação possível e necessária sobre a situação de emergência que lhe é relatada. De acordo com esses dados, o sistema possui a inteligência de decidir quais as entidades que serão envolvidas na ocorrência. Este sistema engloba quatro principais funcionalidades: validação, localização, tipificação e caracterização do incidente (Martins, 2017).

A Figura 3 ilustra o painel de atendimento e processamento das chamadas de emergência, integrado na aplicação de suporte a este atendimento.

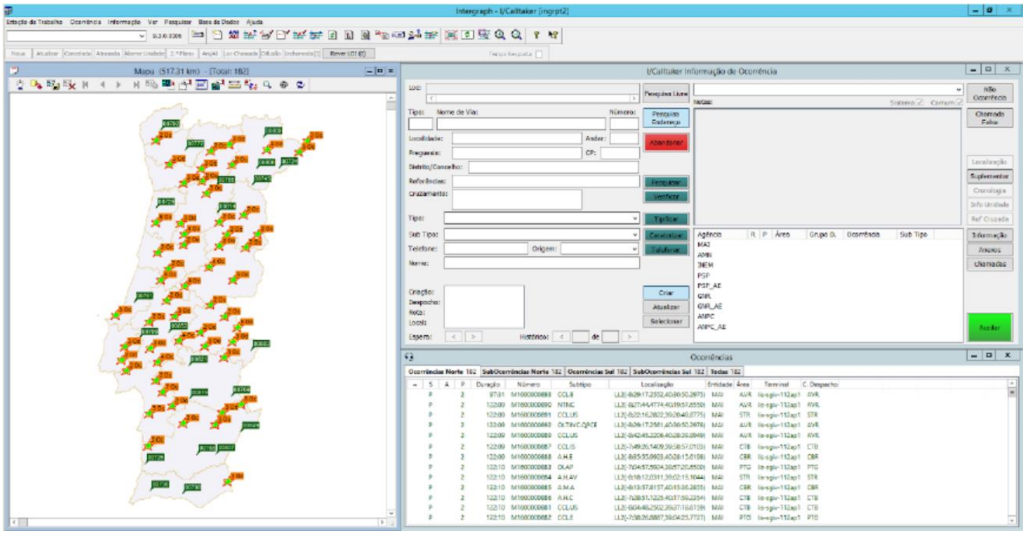


Figura 3 – Consola do operador da central 112 (Martins, 2017)

Como mencionado anteriormente, este operador é frequentemente a primeira de várias linhas de contacto com a vítima de uma emergência médica. Consequentemente, poucos dados pessoais são armazenados ou registados por este centro. Por essa razão, o *software* utilizado inclui apenas campos para registo de informações gerais e abrangentes, como localidade, freguesia, distrito, pontos de referência, contacto de retorno, entre outros dados específicos relacionados com a caracterização da gravidade da ocorrência (Figura 3).

Após este processo, toda a informação recolhida é enviada para as entidades cuja intervenção é necessária, sem prejuízo desses dados poderem vir a ser alterados ou complementados ao longo do tempo (Martins, 2017).

Da informação inicialmente adquirida pelas centrais operacionais, apenas é retornado ao sistema destas centrais 112 o estado de evolução de cada ocorrência por parte de cada uma das entidades envolvidas: Recebido, Recursos Despachados, Recursos no Local e Intervenção Terminada. Esta informação permitirá a produção de relatórios estatísticos e possibilita também a informação do estado de uma ocorrência a cidadãos que contactem as centrais devido a uma situação já reportada (Martins, 2017).

Após a identificação de uma emergência médica por parte das centrais operacionais, o fluxo de atendimento para estes casos prevê, como anteriormente explanado, o direcionamento da chamada inicial para os CODU. Quanto aos equipamentos e sistemas informáticos, estes centros de segunda linha de contacto dispõem de diversos recursos tecnológicos necessários ao cumprimento da sua atividade. Estes instrumentos garantem o registo, a segurança dos dados, e a monitorização e análise de toda a atividade dos CODU (INEM, 2023).

Assim, para o atendimento das chamadas de emergência médica é utilizada a aplicação CMS (*software* de gestão da central telefónica), que regista todo o fluxo de informação referente ao atendimento, permitindo obter informação detalhada do tipo de chamadas, nomeadamente a sua origem (112, SNS24 e os pedidos de triagem dos Corpos de Bombeiros e Delegações da CVP) (INEM, 2023).

De seguida, a triagem das chamadas é efetuada recorrendo a algoritmos de apoio à decisão existentes no sistema - TETRICOSY ®, *TElephonic TRIage and COunseling System*, que se traduz num programa que garante rapidez no tratamento da informação e na decisão de priorizar as vítimas com base nas informações por estas prestadas (INEM, 2023).

No acionamento dos meios de emergência médica, os CODU recorrem à aplicação SIADEM, Sistema Integrado de Atendimento e Despacho de Emergência Médica, que permite tipificar e identificar a localização geográfica das chamadas de emergência recebidas. Além disso, permite ainda, automatizar o despacho de meios, acionando o mais próximo, mais adequado e disponível para o local da ocorrência (INEM, 2023).

Para a comunicação com os meios de emergência, o INEM adotou a nova aplicação *iTeams* (*INEM Tool for Emergency Alert Medical System*), que se traduz num sistema de registo clínico eletrónico nos meios de emergência médica. Desde a sua implementação em 2018, este *software* tem vindo melhorar a articulação entre os meios no terreno, o atendimento efetuado no CODU e as unidades de saúde, melhorando os tempos de chegada ao local da ocorrência e a transmissão de informações em tempo real (INEM, 2023).

Atualmente, este programa é utilizado por 149 corpos de Bombeiros e delegações da CVP num total de 381 meios de emergência médica (INEM, 2024). Estes números evidenciam uma adesão de cerca de 71% para estas entidades, estando os restantes 29% associados à utilização de instrumentos tradicionais, como o papel e a caneta. Nesse contexto, e visto serem estes os dois métodos oficias do INEM para documentação em contexto de terreno, torna-se essencial analisar os campos presentes tanto no programa *iTeams* quanto no verbete nacional de socorro de forma a identificar as informações sensíveis que podem ser recolhidas e registadas durante uma emergência pré-hospitalar.

Após inserção das credenciais pessoais, a equipa de socorro acionada obtém, na primeira página do *software*, uma visualização idêntica à ilustrada pela Figura 4, onde se encontram campos destinados à localização da ocorrência, como o concelho, a freguesia, a rua e, eventualmente, pontos de referência, que permitirão aos profissionais dirigir-se com precisão ao local onde a vítima se encontra.

Além disso, o mesmo ecrã apresenta o fluxo de triagem do CODU, uma área que fornece uma breve descrição contendo as informações essenciais recolhidas pelo operador durante a chamada. Esta funcionalidade permite que as equipas no terreno obtenham uma visão clara e imediata sobre a condição de saúde da vítima e outros detalhes relevantes, facilitando a tomada de decisões rápidas e informadas antes de chegar ao local da ocorrência.

No topo do programa, encontra-se ainda o número do evento CODU, um identificador único atribuído a cada ocorrência. Este número associa diretamente a ocorrência à vítima e

é utilizado para rastrear todo o ciclo de atendimento, desde a triagem inicial até ao encerramento do caso. A utilização desse identificador garante uma organização eficiente das informações, permitindo uma comunicação mais estruturada entre as diferentes entidades envolvidas no processo de socorro.

Figura 4 – Interface da página "Evento" do *software* iTeams (INEM, s.d.)

Após a chegada ao local, e assim que as condições de saúde da vítima o permitirem, a equipa de socorro tem acesso a uma segunda página no sistema, destinada principalmente ao preenchimento dos dados pessoais do utente. Esta interface gráfica, ilustrada na Figura 5, contém diversos campos que permitem a identificação e caracterização da vítima, incluindo nome, género, data de nascimento, idade e morada.

Para agilizar o processo, o sistema possibilita o preenchimento automático destes campos ao introduzir o número de saúde do utente, caso esteja disponível (INEM, s.d.). Essa funcionalidade não só reduz o tempo necessário para registar os dados como também minimiza erros na sua inserção manual.

Além disso, a mesma página apresenta ainda uma janela que exibe o histórico das últimas ocorrências associadas ao utente, fornecendo informações valiosas que podem ser determinantes para a prestação dos cuidados (INEM, s.d.).

Outro campo relevante disponibiliza informações do centro de saúde da vítima, incluindo situações de risco, doenças crónicas ou necessidades específicas, permitindo à

equipa de socorro adaptar a sua abordagem de acordo com as condições preexistentes do paciente (INEM, s.d.). Esta funcionalidade garante uma intervenção mais personalizada e eficaz, alinhada com as necessidades individuais do utente.

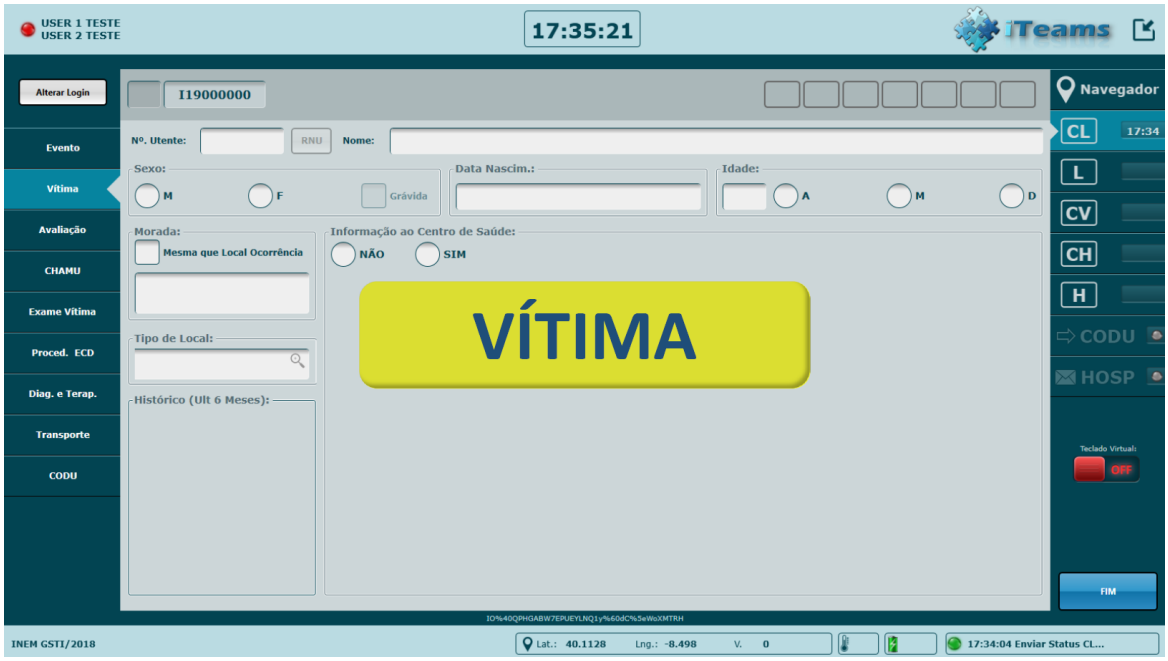


Figura 5 – Interface da página "Vítima" do *software* iTeams (INEM, s.d.)

Após a identificação da vítima, o socorrista deve proceder ao preenchimento dos parâmetros de avaliação clínica, utilizando para isso a terceira página do *iTeams* (Figura 6). Nesta interface, são registados os valores medidos, como frequência cardíaca, temperatura corporal, pressão arterial, entre outros indicadores vitais. Além disso, o sistema permite a caracterização de aspetos visuais importantes, como o comportamento das pupilas e a tonalidade da pele, essenciais para uma avaliação completa do estado de saúde da vítima.

Além disso, a plataforma possibilita o registo de múltiplas avaliações ao longo do socorro, registando cada conjunto de parâmetros em diferentes momentos. Esses dados são automaticamente organizados numa tabela localizada na parte inferior da interface, permitindo um acompanhamento detalhado e estruturado das alterações no estado da vítima. Para facilitar ainda mais a análise, o sistema gera um gráfico dedicado que mostra a evolução dos parâmetros ao longo do tempo, fornecendo uma visão clara e intuitiva que apoia as decisões clínicas da equipa (INEM, s.d.).

Após o preenchimento dos campos, toda a informação registada até ao momento poderá ser enviada para o CODU de forma a possibilitar uma atualização em tempo real sobre o

estado da ocorrência e da vítima (INEM, s.d.). Esta comunicação permite ao CODU acompanhar a evolução da situação e, se necessário, ajustar os recursos mobilizados ou fornecer orientações adicionais à equipa. Além disso, o envio desses dados contribui para preparar as unidades hospitalares para a receção da vítima, garantindo que os profissionais de saúde já disponham de informações essenciais para a continuidade dos cuidados.

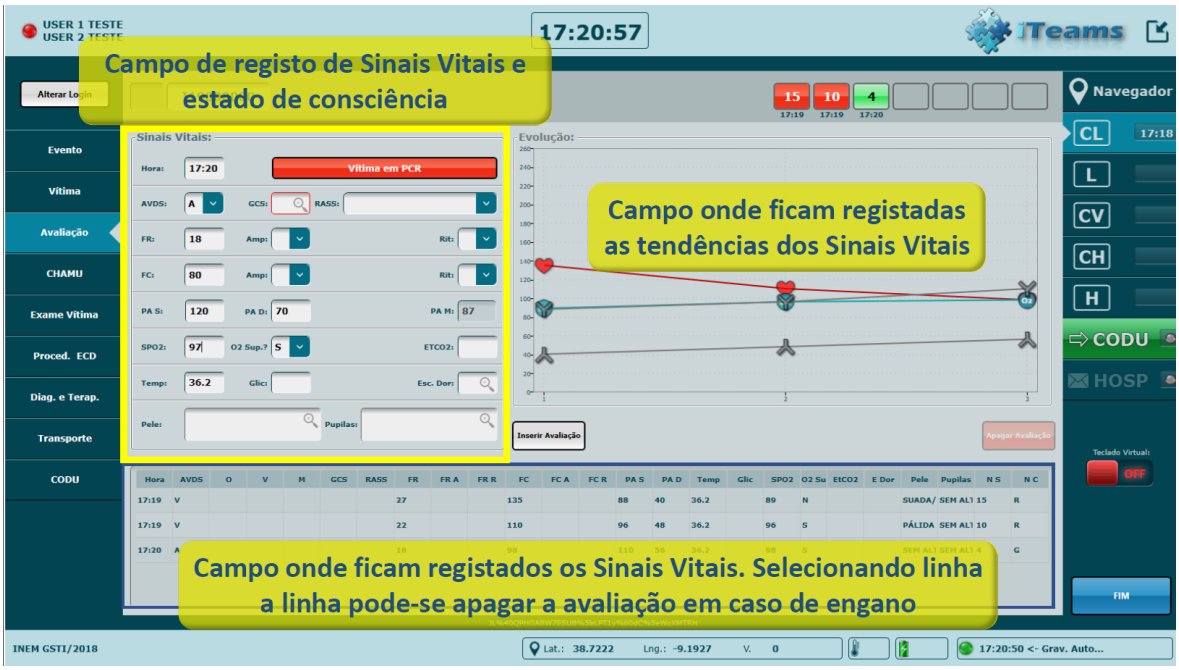


Figura 6 – Interface da página "Avaliação" do *software* iTeams (INEM, s.d.)

Por fim, as duas últimas páginas mais relevantes para o presente estudo são dedicadas à recolha de dados relacionados com a mnemónica CHAMU e o Exame da Vítima. Na primeira (Figura 7), a equipa dispõe de campos específicos para descrever os sintomas e queixas da vítima. Além disso, o sistema permite o registo das circunstâncias associadas ao incidente, do histórico de doenças conhecidas, das alergias, da medicação habitual, bem como do horário e da constituição da última refeição tomada (INEM, s.d.).

Estas informações sensíveis, características de cada vítima, são fundamentais para uma avaliação mais completa e precisa, permitindo aos profissionais compreender melhor o estado clínico e os fatores que podem influenciar a sua condição.

Já na página destinada ao Exame da Vítima, a equipa pode registar as informações obtidas durante a avaliação física, incluindo sinais visíveis de lesão, alterações no estado geral ou outros parâmetros observados diretamente (INEM, s.d.). Estas informações complementam os dados recolhidos anteriormente e oferecem uma visão mais detalhada da

situação clínica da vítima, apoiando não apenas o socorro imediato, mas também a continuidade dos cuidados na unidade hospitalar de destino.

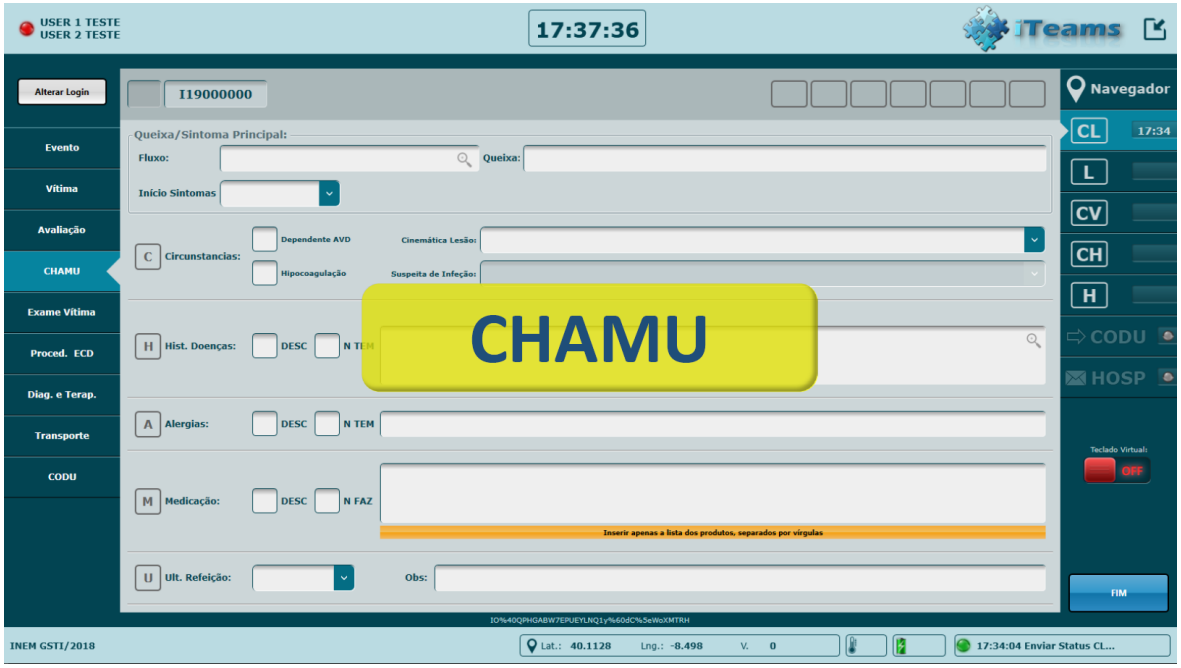


Figura 7 – Interface da página "CHAMU" do *software* iTeams (INEM, s.d.)

As páginas do *iTeams* que se seguem são dedicadas ao registo detalhado de informações essenciais para a conclusão da ocorrência. Estas incluem a descrição dos procedimentos realizados pela equipa de socorro no terreno, a avaliação efetuada pelos profissionais da triagem hospitalar e os possíveis diagnósticos estabelecidos. Além disso, são documentados os protocolos aplicados durante o socorro, os fármacos administrados à vítima e dados relativos ao transporte, como o hospital de destino e a presença ou não de médico, enfermeiro, familiar ou autoridade durante o percurso (INEM, s.d.).

Por fim, o sistema também inclui uma secção que regista o histórico das informações trocadas entre a equipa de socorro e o CODU ao longo da ocorrência (INEM, s.d.). Este histórico pode conter validações de procedimentos realizados, a confirmação do hospital de destino ou o acionamento de meios adicionais de socorro, quando necessário.

Além do *software* informático, muitas vezes, a comunicação entre os CODU ou as centrais e os meios de socorro é estabelecida recorrendo a tecnologias de alta e baixa frequência, como rádios e telemóveis, cada um com características e usos específicos.

Os rádios, por serem rápidos e eficazes, são comumente usados para a comunicação direta e contínua entre os centros de coordenação e os profissionais no terreno. Dada a sua

particular utilidade em situações que exigem, por exemplo, um pedido de reforço de meios, os rádios permitem que as centrais de comando ou apoio diferenciado comuniquem rapidamente com várias unidades, de forma simultânea. Contudo, por serem canais abertos, estes dispositivos táticos não garantem a confidencialidade dos dados transmitidos, o que pode ser um ponto de vulnerabilidade em termos de proteção das informações das vítimas.

Por outro lado, os telemóveis pessoais ou profissionais são, por diversas vezes, utilizados para comunicações que exigem privacidade e segurança das informações transmitidas. Em frequências mais baixas, que permitem uma comunicação privada, os telemóveis são usados para a transmissão de dados sensíveis ou informações detalhadas sobre o estado da vítima que não devem ser compartilhadas através de canais abertos como os utilizados pelos rádios.

Esta diferenciação no uso de tecnologias de comunicação sublinha a importância de adaptar os meios de transmissão às necessidades específicas de cada situação no socorro pré-hospitalar, garantindo tanto a eficácia da resposta quanto a segurança das informações dos titulares dos dados.

De seguida, a menos que haja recusa de transporte por solicitação do utente, direito que lhe é devido, o socorro pré-hospitalar culmina na passagem da vítima para a unidade de saúde. Nestes centros de cuidados hospitalares, são frequentemente utilizados alguns *softwares* para criação de ficha e triagem, que permitem organizar e registar as informações relativas à vítima e ao socorro prestado. Para a primeira tarefa, são apenas registados dados básicos como o número de utente do Serviço Nacional de Saúde (SNS), o tipo de ocorrência, como doença súbita, e a entidade que prestou o socorro. Estas informações são essenciais para associar o episódio ao histórico clínico da vítima e registar a sua entrada na unidade de saúde.

Na triagem, por outro lado, o foco está na recolha de informações clínicas e detalhadas sobre o estado da vítima no momento da admissão. Estes dados incluem sinais vitais, queixas principais, sintomas apresentados e antecedentes médicos relevantes. Sempre que necessário, são também incorporadas informações fornecidas pela equipa de socorro pré-hospitalar sobre as intervenções realizadas e a evolução do quadro clínico até à chegada ao hospital. Este processo é crucial para classificar a gravidade do caso, determinar prioridades de atendimento e garantir que os cuidados sejam prestados de forma célere e adequada à condição do paciente.

Posteriormente, todas as informações recolhidas na triagem são integradas ao sistema interno do centro hospitalar, onde o episódio é armazenado juntamente com resultados de exames médicos, análises clínicas e diagnósticos que venham a ser realizadas ao longo do tratamento do doente.

Em suma, todos estes meios tecnológicos garantem que as etapas do socorro pré-hospitalar estejam devidamente documentadas, promovendo uma continuidade eficaz dos cuidados e a rastreabilidade completa do processo de emergência. No entanto, também alertam para o facto de a recolha e o armazenamento de uma grande quantidade de dados sensíveis exigirem cuidados redobrados com a proteção e a confidencialidade das informações. A gestão inadequada desses dados pode não apenas comprometer a privacidade das vítimas, mas também expor as entidades e os profissionais de socorro a riscos legais e éticos, reforçando a importância de todos os envolvidos conhecerem e cumprirem rigorosamente com as normas de proteção de dados aplicáveis.

3.3.2. Meios tradicionais

Embora os avanços tecnológicos tenham transformado significativamente o sistema de emergência pré-hospitalar, os métodos tradicionais, como o uso de registos físicos, continuam a desempenhar um papel importante em diversas situações. Inicialmente concebidos como a principal forma de documentação, estes métodos foram gradualmente relegados a uma função de apoio, servindo como *backup* em cenários onde a tecnologia enfrenta limitações, como a inacessibilidade aos equipamentos digitais derivado, por exemplo, à falta de bateria ou rede (INEM, s.d.).

No entanto, longe de serem obsoletos, os registos físicos ainda são amplamente utilizados em algumas etapas do socorro, especialmente em contextos onde os recursos tecnológicos não estão disponíveis (INEM, s.d.).

Nas centrais operacionais, onde o atendimento das chamadas depende atualmente de sistemas informatizados para localização e registo, o papel e a caneta são ainda utilizados em situações pontuais, como quando há falhas no sistema ou durante períodos de alta afluência, em que a redundância manual se torna necessária. Assim, as folhas de registo permitem anotar os mesmos dados iniciais da ocorrência, como a morada, o tipo de emergência e o número de vítimas, que posteriormente são transferidos para o sistema assim que este se encontre funcional.

No CODU, onde a triagem e a coordenação são, como anteriormente visto, feitas com o auxílio de *softwares* avançados, as folhas de papel são também utilizadas como uma cópia de segurança em eventos de falha tecnológica. Um exemplo dessa aplicabilidade ocorreu a 27 de novembro de 2024, quando todos os CODU estiveram sem sistema informático durante três horas, obrigando os técnicos a realizar o atendimento de forma manual (Rogado, 2024). Recorrendo a este método tradicional, os profissionais podem de igual forma anotar instruções ou detalhes da ocorrência e enviá-los às equipas de socorro via telefónica, garantindo que a operação não seja interrompida pela indisponibilidade do sistema principal.

A realidade dos meios de socorro no terreno apresenta-se de forma diferente, uma vez que os registos em papel continuam a ser frequentemente a principal ferramenta de documentação em áreas onde a digitalização ainda não foi plenamente implementada ou não é totalmente eficiente. Esta situação é particularmente comum em corporações de Bombeiros que não utilizam sistemas como o *iTeams* ou em casos em que os dispositivos digitais disponíveis estão inoperantes (Erbay, 2014). Nesses cenários, o verbete nacional de socorro em papel encontra-se disponível para todos os meios e parceiros do SIEM, podendo ser requisitado e utilizado para documentar informações de forma padronizada (INEM, s.d.).

A Figura 8 ilustra um exemplo de preenchimento do verbete em papel, que se organiza em várias secções que permitem registar, de forma estruturada, os dados sobre a ocorrência. O verbete é constituído por 3 folhas, cuja original é entregue ao INEM, a duplicada à unidade de saúde ou ao utente, caso rejeite o transporte/tratamento, e a triplicada para o meio de socorro envolvido (INEM, s.d.).

Tal como acontece no *iTeams*, o verbete em papel possui campos equivalentes aos do *software*, abrangendo todas as etapas necessárias para registar a ocorrência. Após receberem informações sobre a localização e o tipo de emergência por parte da central da corporação ou delegação, os meios de socorro deslocam-se ao local onde a vítima se encontra. Quando possível, a equipa deve então recorrer ao verbete e preencher as secções existentes como a localização da ocorrência, a identificação da vítima, a avaliação realizada, o historial clínico, o exame físico e os procedimentos realizados (INEM, s.d.).

Para além de assegurar a documentação essencial, o verbete também cumpre um papel importante no registo legal e na rastreabilidade das ações realizadas pela equipa de socorro. Ao incluir campos destinados a detalhes como fármacos administrados, horários das intervenções e dados sobre o transporte da vítima, o verbete fornece um histórico claro das

decisões e procedimentos adotados. Este registo é particularmente relevante em casos onde é necessário comprovar a conformidade com os protocolos de emergência ou responder a eventuais questões legais ou administrativas relacionadas ao atendimento.

Além disso, o verbete é ainda utilizado como uma referência inicial para os profissionais de saúde da unidade de destino. Ao conter informações sobre a primeira avaliação clínica realizada no terreno, este documento auxilia na continuidade do tratamento, garantindo que os dados fundamentais estejam disponíveis para a equipa hospitalar no momento da triagem.

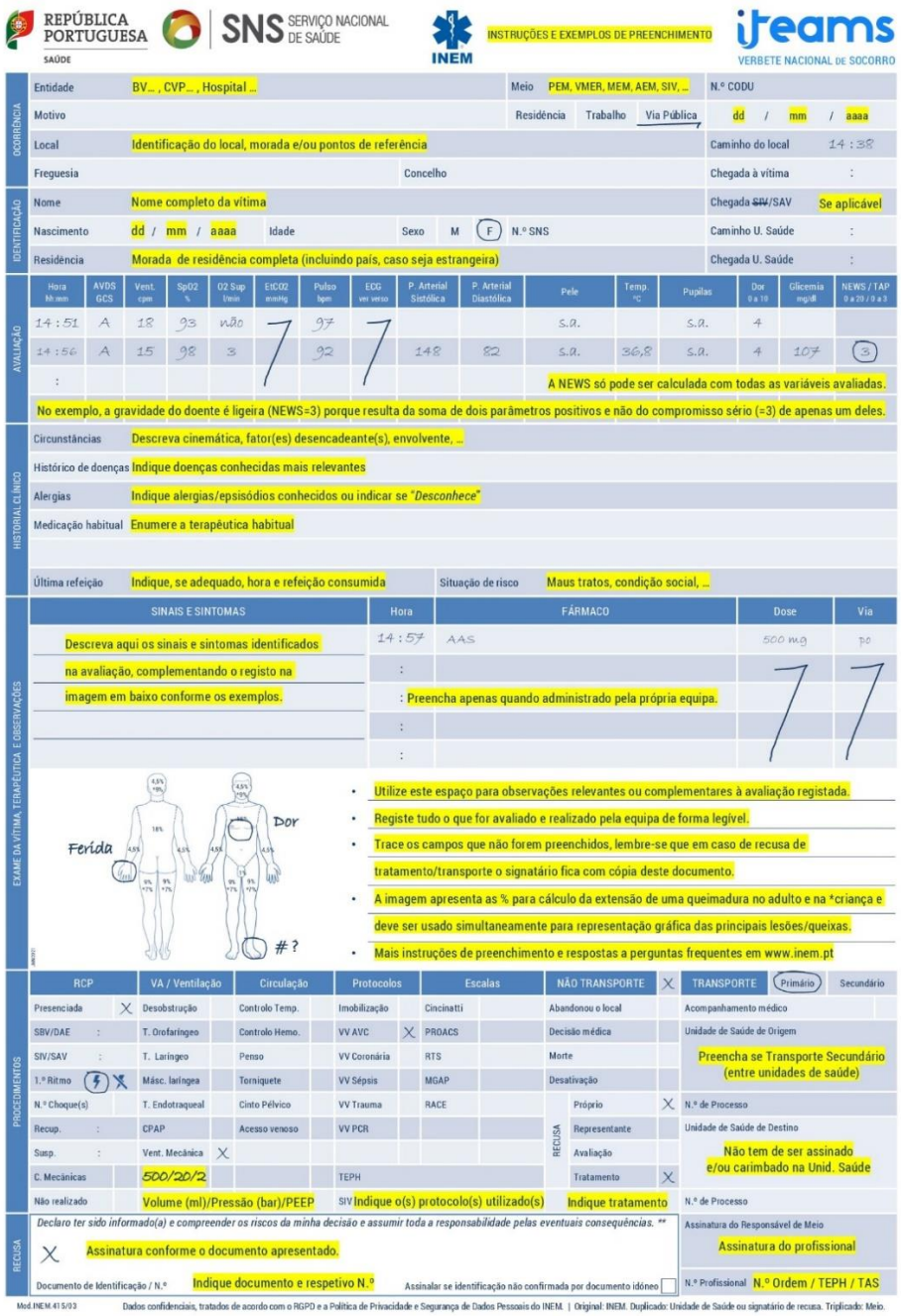


Figura 8 – Exemplo de preenchimento do Verbete Nacional de Socorro (INEM, s.d.)

Por fim, à semelhança dos centros operacionais, e embora a maioria das unidades esteja equipada com sistemas digitais para triagem e criação de fichas de paciente, o uso de papel nos serviços de urgências ainda pode ocorrer em situações específicas, como durante picos de afluência em que o sistema informatizado apresente lentidão ou indisponibilidade. Além disso, as cópias dos documentos manuais preenchidos pelas equipas de socorro, como os verbetes, podem ser entregues ao unidade de cuidados no momento da admissão da vítima, servindo como um complemento ou reforço das informações transmitidas oralmente.

Em resumo, apesar das limitações em relação aos sistemas digitais, a simplicidade e a universalidade do verbete e dos restantes meios tradicionais tornam estas ferramentas confiáveis em qualquer contexto, especialmente em situações onde a tecnologia não está disponível. No entanto, enquanto os sistemas e programas informáticos podem garantir a segurança dos dados através da implementação de medidas de segurança nos servidores e nas unidades de armazenamento das entidades envolvidas, o uso de documentação física exige a adoção de medidas adicionais que assegurem a proteção e a confidencialidade das informações sensíveis das vítimas.

3.4. Situações de acesso aos dados armazenados

Após o encerramento de qualquer ocorrência, o acesso aos dados das vítimas continua a ser necessário para diversas finalidades, tanto operacionais quanto administrativas. A preservação e conservação dos dados clínicos/nominativos obtidos no âmbito da assistência prestada, são da responsabilidade do INEM, podendo ser facultados ao respetivo titular e/ou a terceiros, nos casos legalmente previstos. O seu acesso, designadamente a documentos administrativos que incluam dados de saúde, encontra-se regulado pela Lei N.º 46/2007, de 24 de agosto, que aprovou a Lei do Acesso aos Documentos Administrativos (LADA) (INEM, s.d.).

Nesse sentido, a nível de utilidade dessas informações, as mesmas poderão ser especialmente acedidas em quatro principais contextos:

1. **Consulta pelo titular dos dados:** A própria vítima pode, em determinados casos, solicitar acesso às informações registadas sobre uma ocorrência em que foi atendida. Este direito, garantido pela legislação, permite que o indivíduo tenha conhecimento sobre como os seus dados foram tratados, incluindo informações recolhidas, intervenções realizadas e eventuais partilhas com outras entidades (INEM, s.d.);

2. **Consulta do histórico clínico:** Os dados armazenados em equipamentos e programas informáticos permitem que os profissionais de emergência pré-hospitalar ou hospitalar acedam ao histórico clínico de uma vítima. Este acesso poderá ser essencial para obter informações relevantes em futuras emergências, como intervenções anteriores, sinais vitais habituais e condições médicas conhecidas. Desta forma, torna-se possível a personalização do tratamento e a otimização da resposta em novas ocorrências envolvendo cada vítima (INEM, s.d.);

3. **Fins legais/judiciais:** Em algumas situações, as informações recolhidas durante o socorro podem ser consultadas para responder a investigações judiciais relacionadas ao incidente. Nesses casos, os dados servem como documentação oficial do socorro prestado, ajudando a esclarecer factos e a cumprir exigências legais (INEM, 2017);

4. **Elaboração de relatórios estatísticos:** As informações das ocorrências podem também ser utilizadas para a análise de dados e elaboração de relatórios periódicos por parte das entidades envolvidas, que avaliam o desempenho dos serviços de emergência e identificam tendências relacionadas às ocorrências. Esses relatórios e estudos são fundamentais para o planeamento e a melhoria contínua dos serviços, além de servirem como base para decisões estratégicas e investimentos em recursos.

Assim, para aceder a informações relacionadas a pedidos de auxílio no âmbito da emergência médica, encaminhados ou tratados pelo INEM, é necessário o preenchimento de um formulário específico disponibilizado para esse propósito. Este documento reúne diversas áreas, incluindo a da identificação do requerente, identificação do titular dos dados, legitimação do pedido, informações solicitadas, identificação da ocorrência, detalhes de intermediação médica, finalidade do pedido e forma de acesso desejada. O formulário deve ser devidamente preenchido e enviado ao INEM através dos canais oficiais (INEM, s.d.).

Adicionalmente, a Figura 9 apresenta um quadro publicado pelo INEM que detalha os documentos necessários para anexar ao pedido, dependendo da entidade ou do indivíduo que solicita o acesso aos dados. Este recurso visa garantir a conformidade do processo, assegurando que apenas pedidos legítimos e devidamente justificados sejam considerados (INEM, 2017).

A análise da mesma figura revela a diversidade de autorizações e documentos necessários para que o acesso aos dados seja concedido. Dependendo da natureza do

requerente, são exigidos diferentes comprovativos e justificações, que garantem o cumprimento das normas de tratamento e proteção de dados e a salvaguarda da privacidade das vítimas.

		Origem do pedido de acesso a dados						
		Titular	Titular - menor e/ou incapaz	Terceiros	Advogados	Seguradoras	Autoridades	
							Policiais	Judiciárias
Informações/documentos necessários	Requerimento	X	X	X	X	X	X	X
	Documento identificativo do requerente e do titular	X	X	X	X	X		
	Documento comprovativo da legitimidade		X[1]		X[2]			
	Autorização escrita do titular dos dados			X[3]		X[4]		
	Prova do Interesse						X	
	Identificação do nº de processo			X[5]	X[5]		X	X

Figura 9 – Documentos necessários para pedido de acesso a dados de ocorrências (INEM, 2017)

Independentemente da finalidade, é crucial que o acesso aos dados seja restrito, monitorizado e realizado em conformidade com as normas de proteção de dados, uma vez que garantir a segurança e a confidencialidade das informações é indispensável para proteger a privacidade das vítimas e manter a confiança nos serviços de emergência.

Assim sendo, torna-se essencial conhecer e compreender o enquadramento normativo em vigor, de modo a assegurar que todas as equipas de socorro envolvidas conheçam e cumpram com as suas obrigações legais e éticas antes, durante e após qualquer ocorrência.

3.5. Mecanismos de segurança existentes

Devido à natureza sensível das informações de saúde, aliada à imprevisibilidade das situações de emergência, torna-se fundamental que todos os sistemas, programas ou equipamentos envolvidos contem com mecanismos de segurança robustos. Estes mecanismos devem proteger os dados dos titulares e assegurar a continuidade das operações de socorro, minimizando qualquer possível interrupção na prestação de cuidados urgentes.

Neste contexto, o INEM, como organismo do Ministério da Saúde responsável pela coordenação do funcionamento do SIEM no território continental português, fundamenta a sua política de segurança da informação nos princípios de confidencialidade, integridade e disponibilidade. Estes pilares visam garantir a proteção contra o acesso não autorizado à informação, a correção e completude dos dados, e o acesso continuado às informações necessárias para as operações (INEM, 2022).

Com base nisso, a entidade adota princípios transversais que contribuem para a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) adequado, tais como (i) Acesso condicionado ao desempenho, (ii) Não dependência do secretismo, (iii) Segurança em profundidade, (iv) Segregação de funções, (v) Proporcionalidade, (vi) Homogeneidade, (vii) Resiliência e (viii) Manutenção da confiança (INEM, 2022).

Além do mais, o INEM comprometeu-se, no passado ano de 2024, a proteger a informação recebida, produzida, transmitida, armazenada e processada contra a perda de qualquer um dos três princípios de segurança. Para isso compromete-se a desenvolver e implementar, de acordo com as melhores práticas nacionais e internacionais, políticas e procedimentos técnicos e específicos para as diferentes áreas de intervenção na estrutura do instituto. Esta política foi formalmente aprovada pelo Conselho Diretivo do INEM, demonstrando o interesse do mesmo em que as operações de emergência sejam realizadas com a máxima segurança e eficiência (INEM, 2022).

De forma concreta, na alínea 8 da Política de Privacidade e Proteção de Dados Pessoais, o INEM declara que assegura o cumprimento da legislação aplicável, através da adoção de normas específicas de Segurança dos Sistemas e Tecnologias de Informação (INEM, 2018). Essas normas caracterizam-se como um conjunto de tecnologias e procedimentos de segurança que a entidade de saúde considera adequadas à proteção dos dados sensíveis contra acessos e divulgações não autorizados. Essas medidas refletem-se quer em processos automatizados, quer em processos manuais, nomeadamente:

- **Segurança física:** Como o controlo de acessos de trabalhadores, colaboradores e visitantes às instalações, mecanismos restritos de combate à intrusão nos sistemas de informação, extinção de incêndios, monitorização de equipamentos em regime 24×7 e alojamento de serviços em bastidores próprios (INEM, 2018);
- **Segurança lógica:** Na componente de acessos a sistemas e dispositivos através de mecanismos de gestão de identidades, autenticação e perfis de acesso. Na componente de rede através do uso de *firewalls* e sistemas de deteção de intrusão, segregação de redes e ambientes aplicacionais, bem como cifragem de informação através de canais de comunicação seguros (INEM, 2018).

Apesar de, usualmente, os corpos de Bombeiros e delegações da CVP não operarem como centrais de atendimento de chamadas de emergência médica, estas entidades lidam de igual forma com uma quantidade considerável de informação sensível, tanto durante o

socorro quanto na subsequente documentação e armazenamento de dados, como é o caso dos verbetes. Nesse sentido, é também fundamental que adotem medidas adequadas de proteção de dados, embora estas possam não precisar de ser tão rigorosas quanto as exigidas ao INEM. Ainda assim devem ser suficientemente robustas para assegurar a confidencialidade e segurança da informação manipulada.

Atualmente, a adoção dessas medidas de Cibersegurança varia significativamente entre as instituições humanitárias, uma vez que a implementação de tais normas depende largamente da capacidade de investimento e dos recursos disponíveis de cada associação. Acredita-se que, nas entidades com maior conforto financeiro, devido, por exemplo, à possível existência de doações e financiamentos regulares de altos valores, a segurança da informação consiga ser uma prioridade, possibilitando a adoção práticas como a encriptação de dados, o controlo de acessos rigorosos e a formação contínua sobre práticas seguras de gestão de informação entre funcionários e voluntários.

No entanto, é também possível especular que na maioria das instituições, especialmente as mais antigas ou com menos recursos, possam ter deficiências significativas na consciencialização e formação dos profissionais de saúde e do pessoal administrativo e na implementação de medidas de segurança robustas, expondo os dados das vítimas a um maior nível de risco de acessos não autorizados e violações de dados.

Também na chegada às unidades hospitalares, a existência de cuidados com a privacidade da vítima torna-se crucial. Assim, durante o processo de admissão à urgência, os profissionais iniciam a criação de uma ficha para a vítima. Nesta primeira etapa, são apenas fornecidos dados como o número do SNS da vítima e o motivo de admissão, facilitando a identificação e o encaminhamento preliminar. Posteriormente, durante a triagem, ocorre a transmissão de informações pessoais e de saúde mais detalhadas, que requerem um nível elevado de confidencialidade. Por esta razão, a triagem é frequentemente realizada em espaços individuais e privados internos ao edifício, assegurando a privacidade das informações transmitidas.

Com o desenvolvimento deste estudo, pretende-se que, apesar da existência dessas dificuldades, todos os parceiros do SIEM consigam desenvolver e manter uma política de privacidade e proteção de dados interna que atenda às necessidades específicas da sua operação, mas que, ao mesmo tempo, garanta o cumprimento da legislação em vigor, que passa agora a ser explorada.

4. Enquadramento normativo

A privacidade e a proteção de dados pessoais ocupam, cada vez mais, um lugar central na sociedade contemporânea, especialmente face aos avanços tecnológicos e à digitalização das informações. A necessidade de regulamentar a vida privada, garantindo o respeito pela intimidade de cada indivíduo, não é um conceito moderno. Desde a Antiguidade, civilizações como a grega já reconheciam a importância da convivência em sociedade e da salvaguarda de aspetos íntimos, ainda que de forma rudimentar.

Com o passar dos séculos, o conceito de privacidade evoluiu e ganhou novos contornos, principalmente com o surgimento de tecnologias que ampliam a capacidade de recolha, armazenamento e partilha de informações pessoais. A área da saúde, em particular, destaca-se pela sua sensibilidade, já que lida com dados íntimos e muitas vezes críticos para o bem-estar das pessoas. Assim, garantir a proteção desses dados não é apenas uma questão ética, mas também legal, sendo essencial estabelecer normas que assegurem a confidencialidade e a segurança das informações em todos os contextos, incluindo o da emergência pré-hospitalar.

Nesse sentido, o presente capítulo apresenta vários instrumentos legislativos e regulamentares que moldaram o panorama da proteção de dados pessoais, com foco na área da saúde.

Numa primeira abordagem, a Tabela 1 fornece uma visão cronológica e abrangente dos principais documentos que caracterizaram a evolução do tratamento e da proteção de dados em território europeu e português, através do estabelecimento de padrões e diretrizes aplicáveis até aos dias de hoje.

Para cada documento listado, a tabela especifica o ano de adoção ou promulgação, o título completo, uma breve descrição do seu conteúdo e propósito principal, e uma indicação relativa à atual vigência ou revogação do respetivo documento.

Esta organização cronológica e descritiva permite não só compreender a evolução das normas de proteção de dados ao longo do tempo, mas também identificar os marcos regulatórios que continuam a influenciar as práticas atuais no tratamento de dados sensíveis, garantindo uma referência rápida e informativa para a contextualização normativa no estudo em curso.

Tabela 1 – Evolução do quadro normativo (europeu e português) por data de publicação

Ano	Título	Descrição	Vigente?
400 a.C.	Juramento de Hipócrates	Fundamento ético que estabelece o princípio do segredo médico (Wikipedia, 2024)	Não aplicável
1948	Declaração Universal dos Direitos do Homem	Documento que reconhece o direito à proteção contra interferências arbitrárias na vida privada, sendo um marco inicial na defesa da privacidade como direito humano (Nações Unidas [NU], s.d.)	Sim
1950	Convenção Europeia dos Direitos do Homem (CEDH)	Tratado que garante o direito ao respeito pela vida privada e familiar, com proteção específica contra interferências do Estado ou de terceiros (Conselho da Europa [CE], s.d.)	Sim
1970	Lei moderna de privacidade (Alemanha)	Introdução da primeira lei moderna de proteção de dados, regulamentando o uso de dados pessoais e estabelecendo princípios para a sua gestão ética e legal (Carvalho et al., 2019), (Osswald, 1970)	Não
1973	Resolução 73/22 do Conselho da Europa	Recomendação inicial sobre proteção de dados pessoais em sistemas informatizados no setor privado (CE, 1973)	Não
1974	Resolução 74/29 do Conselho da Europa	Complementa a anterior, incluindo princípios para tratamento e proteção de dados pessoais no setor público (CE, 1974)	Não
1973/ 1974	*Data Act* (Suécia)	Primeira lei nacional de privacidade, estabelecendo regras específicas para o tratamento de dados pessoais na Suécia (Wikipedia, 2024)	Não
1976	Artigo 35º da Constituição da República Portuguesa	Garante proteção contra o uso abusivo de dados pessoais e o uso da informática de forma a respeitar a dignidade humana (Assembleia República [AR], 1976)	Sim
1980	Guidelines da OCDE	Diretrizes sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais, criando padrões globais para o tratamento ético de informações (OCDE, 2022)	Não vinculativo
1981	Convenção 108 do Conselho da Europa	Primeiro tratado internacional vinculativo em proteção de dados, estabelecendo padrões para os Estados-Membros (CE, 1981)	Sim
1995	Diretiva 95/46/CE	Estabeleceu os princípios básicos de proteção de dados na União Europeia, exigindo que os Estados-Membros adaptassem as suas legislações nacionais (União Europeia [UE], 1995)	Não

1997	Declaração Universal sobre o Genoma Humano e Direitos Humanos	Declaração adotada pela UNESCO que aborda questões éticas, legais e sociais relacionadas ao genoma humano. Enfatiza a importância de proteger a dignidade humana e os direitos humanos, incluindo a privacidade e a confidencialidade dos dados genéticos (UNESCO, 2001)	Não vinculativo
1998	Lei nº 67/98, de 26 de Outubro	Transpôs para Portugal a Diretiva 95/46/CE, estabelecendo regras para o tratamento de dados pessoais e proteção dos direitos fundamentais de privacidade (AR, 1998)	Não
2000	Carta dos Direitos Fundamentais da UE	Reconhece a proteção de dados pessoais como um direito fundamental no artigo 8º, consolidando a sua importância no ordenamento jurídico europeu (UE, 2012)	Sim
2001	Protocolo Adicional à Convenção 108	Introduz garantias adicionais relacionadas a autoridades de supervisão e fluxos transfronteiriços de dados pessoais (CE, 1981)	Sim
2002	Diretiva 2002/58/CE	Relativa ao tratamento de dados pessoais e à proteção da privacidade nas comunicações eletrónicas, também conhecida como Diretiva *ePrivacy* (EU, 2002)	Sim
2003	Declaração Internacional sobre os Dados Genéticos Humanos	Declaração que visa garantir a proteção dos dados genéticos humanos, especialmente no que diz respeito à recolha, armazenamento e uso desses dados. Reforça o direito à privacidade e a necessidade de consentimento informado para o uso de informações genéticas (UNESCO, 2004)	Não vinculativo
2004	Lei nº 41/2004, de 18 de Agosto	Regulamenta a proteção de dados no setor das comunicações eletrónicas, alinhada com a Diretiva 2002/58/CE (*ePrivacy*) (AR, 2004)	Sim
2005	Lei nº 12/2005, de 26 de Janeiro	Estabelece regras específicas para o tratamento de informação genética e dados de saúde, com foco em confidencialidade e acesso a pessoal autorizado (AR, 2005)	Sim
2007	Tratado de Lisboa	Reforçou a proteção de dados como direito fundamental da União Europeia, consolidando o artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) (UE, 2007)	Sim
2007	Lei nº 46/2007, de 24 de Agosto	Define o acesso a documentos administrativos em Portugal, incluindo regras sobre o tratamento de dados pessoais contidos nesses documentos (AR, 2007)	Sim
2010	Deliberação nº 629/2010 da CNPD	Define orientações específicas para a proteção de dados no setor da saúde, incluindo o acesso e partilha de informações clínicas (Roque *et al.*, 2007)	Sim

2011	Diretiva 2011/24/UE	Relativa à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços, abordando a proteção de dados de saúde no contexto da mobilidade de pacientes na UE (UE, 2011)	Sim
2013	Resolução 68/167 da Assembleia Geral das Nações Unidas	O "Direito à privacidade na era digital" é um marco internacional que reforça o direito à privacidade em contextos digitais (NU, 2014)	Não vinculativo
2014	Regulamento Delegado (UE) nº 1042/2014	Relativo às normas técnicas mínimas para proteção de informações e dados em sistemas de saúde eletrónicos, reforçando requisitos para entidades que armazenam e processam dados de saúde (UE, 2014)	Sim
2016	Regulamento (UE) 2016/679 (RGPD)	Regulamento Geral sobre a Proteção de Dados, aplicável diretamente em todos os Estados-Membros, estabelecendo normas robustas de proteção e direitos dos titulares (UE, 2016)	Sim
2017	Despacho n.º 1348/2017	Reforça as competências da SPMS (Serviços Partilhados do Ministério da Saúde) no contexto da privacidade dos dados no setor da saúde em Portugal (GSES, 2017)	Sim
2019	Lei nº 58/2019, de 8 de Agosto	Regulamentou o RGPD em Portugal, adaptando a legislação nacional às disposições europeias (AR, 2019)	Sim
2019	Lei nº 59/2019, de 8 de Agosto	Transpõe a Diretiva 2016/680, regulando o tratamento e a proteção de dados no âmbito da prevenção, investigação e repressão de infrações penais e execução de sanções penais (AR, 2019)	Sim
2021	Proposta do Espaço Europeu de Dados de Saúde	Iniciativa da CE para estabelecer um quadro regulamentar que facilite a partilha segura de dados de saúde para cuidados, investigação e políticas públicas (UE, 2022)	Sim
2022	Diretiva 2022/2555 (NIS2)	Foca-se na Cibersegurança e inclui entidades de saúde como parte dos setores críticos que devem proteger dados sensíveis contra incidentes de segurança (UE, 2022)	Sim

A dimensão da Tabela 1 evidencia a extensa história dos documentos legislativos e regulamentares dedicados à proteção de dados, destacando a frequência crescente da sua criação e revisão, especialmente desde o início do século XXI. Este aumento de produção normativa reflete a influência de fatores já abordados como o rápido desenvolvimento tecnológico, a globalização da informação e uma consciencialização crescente sobre a importância da privacidade dos dados.

É ainda de notar que diversos documentos foram sendo revogados ao longo do tempo devido às novas necessidades da sociedade e ao surgimento de tecnologias que exigiram abordagens regulatórias mais robustas e adaptadas aos desafios.

Prosseguindo com uma análise mais detalhada, o presente capítulo encontra-se estruturado em dois subcapítulos distintos, focando separadamente no direito europeu e no direito nacional. Esta divisão estratégica permite uma exploração minuciosa das legislações e regulamentações mais significativas atualmente em vigor. Ao examinar especificamente as normas mais influentes, pretende-se facilitar a compreensão das dinâmicas normativas em cada contexto, destacar como as regulamentações europeias moldam o quadro legal português, e ainda ajudar à perceção de como cada norma virá a ser efetivamente implementada na prática para proteger os dados pessoais das vítimas em situações de emergência.

4.1. Direito europeu

Como visto anteriormente, a construção de um quadro normativo europeu para a proteção de dados pessoais e de saúde reflete um longo processo histórico e jurídico que acompanhou as transformações tecnológicas e sociais do continente e de todo mundo. Desde os primeiros instrumentos que abordaram a privacidade como um direito humano fundamental, até à consolidação de regulamentos específicos para o tratamento de dados em setores sensíveis, como a saúde, o direito europeu tem evoluído de forma a responder aos desafios impostos pela modernidade.

O progresso neste domínio foi marcado pela adoção de declarações e convenções que estabeleceram os princípios básicos da proteção de dados, passando por diretivas e regulamentos que harmonizam práticas entre os Estados-Membros da União Europeia. Além disso, os instrumentos legislativos e regulamentares do Conselho da Europa desempenharam um papel crucial na definição de padrões mínimos de proteção, influenciando diretamente a legislação europeia.

Neste subcapítulo, é novamente analisada a evolução normativa europeia de forma cronológica, porém focando agora nos principais documentos que têm moldado o tratamento e a proteção de dados pessoais, particularmente no setor da saúde e em contextos de emergências pré-hospitalares. Para tal foram selecionados documentos-chave com base em critérios de relevância prática, impacto regulatório direto e influência contínua nas

legislações nacionais. Esta seleção criteriosa permite destacar como o direito europeu estabelece a base para legislações nacionais e contribui substancialmente para a proteção dos direitos fundamentais dos cidadãos em situações críticas.

4.1.1. Declaração Universal dos Direitos do Homem

Adotada pela Organização das Nações Unidas em 10 de dezembro de 1948, a Declaração Universal dos Direitos do Homem estabelece os direitos fundamentais de todos os seres humanos, e a sua relevância no presente estudo é observada em vários artigos, especialmente no que diz respeito à privacidade e ao tratamento de informações pessoais (NU, s.d.).

No contexto da proteção da privacidade do indivíduo, o Artigo 12.º destaca que: "*Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.*" (NU, s.d.).

Já os Artigos 19.º e 27.º garantem, respetivamente, a liberdade de expressão e o direito ao acesso e benefício do progresso científico. No contexto da saúde, este primeiro assegura que os indivíduos possam comunicar informações sobre a sua saúde sem interferências indevidas, enquanto o segundo artigo reforça o direito de todos a usufruir dos avanços científicos, como tratamentos médicos, destacando a importância de tratar dados de saúde de forma ética e segura para promover o bem-estar coletivo (NU, s.d.).

Desta forma, a declaração forneceu uma base ética e legal para a criação de instrumentos específicos que a sucederam, como a Convenção Europeia dos Direitos do Homem, sustentada pela ideia de que o respeito à vida privada é um direito humano inalienável.

4.1.2. Convenção Europeia dos Direitos do Homem

Cerca de dois anos após a publicação da anterior declaração, o Conselho da Europa veio a adotar a Convenção Europeia dos Direitos do Homem (CEDH): um tratado juridicamente vinculativo que estabelece direitos e liberdades fundamentais para os Estados signatários.

No âmbito das exceções ao direito à vida privada, a convenção destaca o Artigo 8.º, que dispõe: "*1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir*

uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros." (CE, s.d.).

Assim, este artigo serve como base para proteger a confidencialidade de informações sensíveis, garantindo que a recolha, o tratamento e o acesso aos dados de saúde sejam estritamente regulados. No setor da saúde, onde os dados das utentes são particularmente sensíveis, o Artigo 8.º reforça a necessidade de que esses direitos fundamentais sejam respeitados e que qualquer exceção seja devidamente justificada (CE, s.d.).

À semelhança da declaração anterior, a Convenção Europeia dos Direitos do Homem veio também a influenciar diretamente a elaboração de outros instrumentos jurídicos relevantes, como a Convenção 108 do Conselho da Europa e o Regulamento Geral sobre a Proteção de Dados. Ambos os documentos reforçam a importância de proteger a privacidade e a confidencialidade das informações pessoais, consolidando os princípios estabelecidos pela CEDH e adaptando-os às exigências da era digital.

4.1.3. Convenção 108 do CE

Ratificada em 1981, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais, conhecida como Convenção 108, foi o primeiro tratado internacional a estabelecer regras vinculativas para proteção de dados pessoais. A relevância desta Convenção no contexto da proteção de dados de saúde é evidenciada em vários dos seus artigos, particularmente em relação à privacidade e ao tratamento ético de informações pessoais (CE, 1981).

Numa primeira fase, o documento aborda a qualidade das informações (Artigo 5.º), definindo que: "*Os dados pessoais objeto de tratamento automatizado devem ser: obtidos de forma justa e legal, e armazenados de forma que permitam a identificação dos interessados apenas durante um período não superior ao necessário para a realização dos objetivos para os quais esses dados foram recolhidos ou tratados posteriormente.*" (CE, 1981). Transpondo as alíneas deste artigo para o contexto da emergência pré-hospitalar, a minimização do tempo de armazenamento de dados pessoais deverá ser objeto de especial atenção e proteção, evitando o uso indevido ou exposição desnecessária de informações sensíveis relativas à vítima ou à ocorrência.

De seguida, o Artigo 6.º trata de forma específica as categorias especiais de dados, estipulando que: "*Dados pessoais que revelem a raça, a política, as convicções religiosas ou outras, bem como os dados pessoais relativos à saúde ou à vida sexual, só podem ser objeto de tratamento automatizado se o direito interno prever garantias adequadas.*" (CE, 1981). Através deste artigo, ressalta-se a necessidade de garantias adicionais ao lidar com dados de saúde, exigindo que sistemas como os usados na emergência médica implementem medidas de Cibersegurança rigorosas para proteger informações sensíveis.

De forma idêntica, o Artigo 7.º reforça o aspeto prático da segurança dos dados, estabelecendo que: "*As medidas de segurança apropriadas devem ser tomadas para a proteção dos dados pessoais armazenados ou tratados, de forma a prevenir qualquer destruição acidental ou ilegal, perda acidental, alteração, divulgação ou acesso não autorizado, em particular quando o processamento envolve a transmissão de dados através de uma rede, e contra todas as outras formas ilícitas de tratamento.*" (CE, 1981). Esta norma torna-se particularmente relevante para o tema em estudo, uma vez que sublinha a importância da adoção de procedimentos e medidas que evitem acessos não autorizados a todo e qualquer meio físico ou digital que armazene ou trate dados pessoais de terceiros.

Por fim, o Artigo 8.º, diz respeito a "Salvaguardas adicionais para o titular dos dados", garantindo direitos fundamentais ao acesso e controlo sobre os próprios dados pessoais. Este artigo permite que qualquer pessoa possa: "*a) confirmar se os seus dados estão a ser processados e para quais fins, além de identificar o responsável pelo arquivo; b) obter acesso aos seus dados armazenados em forma inteligível, sem demora ou custo excessivo; c) solicitar a retificação ou apagamento dos seus dados (...); d) obter uma solução caso os seus pedidos de acesso, retificação ou apagamento não sejam atendidos*" (CE, 1981). Foi através deste oitavo artigo que a Convenção 108 introduziu, pela primeira vez, princípios inovadores para a proteção de dados, estabelecendo alicerces que foram posteriormente expandidos e detalhados por diversas regulamentações da União Europeia, como o RGPD. Assim, esta norma assegura que os indivíduos possam verificar o processamento dos seus dados pessoais, aceder e corrigir essas informações, reforçando a transparência e o controlo pessoal sobre os próprios dados.

Todos estes artigos estabeleceram uma base legal mais específica para a proteção dos dados pessoais, delineando algumas das responsabilidades e direitos essenciais que formam o núcleo da Cibersegurança na atualidade.

4.1.4. Carta dos Direitos Fundamentais da UE

Promulgada em 2000 e juridicamente vinculativa desde a entrada em vigor do Tratado de Lisboa em 2009, a Carta dos Direitos Fundamentais da União Europeia é um instrumento normativo que enuncia e garante uma gama abrangente de direitos e liberdades civis, políticos, económicos e sociais para os cidadãos da UE (EU, 2012). No que toca especificamente à privacidade e proteção de dados, este documento lista dois relevantes artigos: 7.º e 8.º.

No primeiro, intitulado "Respeito pela vida privada e familiar", é descrito que "*Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.*" (EU, 2012). Este artigo reforça uma vez mais a importância de proteger a privacidade individual em todas as circunstâncias, refletindo um valor central mantido consistentemente ao longo das evoluções legais europeias.

Já no segundo, aborda-se a proteção de dados pessoais, através das seguintes alíneas: "*1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.*" (EU, 2012). Com estas declarações, o artigo oitavo reforça a estrutura de proteção de dados pessoais ao afirmar, de forma concisa, princípios já estabelecidos anteriormente, como a necessidade de tratamento justo e específico dos dados pessoais. Além disso, na segunda alínea introduz-se o conceito de consentimento, marcando a primeira vez que a autorização do titular de dados é formalmente requerida e destacada como uma pedra angular na proteção de dados pessoais. Assim, esta inovação foi crucial para o desenvolvimento subsequente do quadro normativo, marcando um avanço significativo na forma como o consentimento é percebido e tratado dentro do direito europeu.

4.1.5. Diretiva 2002/58/CE

Também conhecida como Diretiva *e-Privacy*, a Diretiva 2002/58/CE foi adotada pelo Parlamento Europeu e pelo Conselho da União Europeia a 12 de julho de 2002, com o objetivo de complementar a revogada Diretiva 95/46/CE, estabelecendo normas mais específicas para a privacidade e proteção de dados pessoais no setor das comunicações eletrónicas. Este novo documento permite garantir que os avanços tecnológicos na área das telecomunicações não comprometam o direito fundamental à privacidade e à proteção de

dados, especialmente em relação à integridade das comunicações, à confidencialidade dos dados de tráfego e ao uso de informações de localização (EU, 2002).

Uma das primeiras novidades introduzidas por esta diretiva encontra-se no seu Artigo 2.º, que estabelece as definições fundamentais utilizadas ao longo do documento. Entre estas, destaca-se a introdução da alínea f), onde se especifica que: "*"Consentimento" por parte do utilizador ou assinante significa o consentimento dado pela pessoa a quem dizem respeito os dados, previsto na Directiva 95/46/CE.*" (EU, 2002). Com esta definição, a diretiva reforça a necessidade de que qualquer tratamento de dados pessoais no âmbito das comunicações eletrónicas seja feito com o consentimento expresso do titular, garantindo assim uma maior salvaguarda dos direitos dos indivíduos (EU, 2002). Este conceito, tal como abordado anteriormente na Carta dos Direitos Fundamentais da UE, representa um passo importante na evolução da proteção da privacidade, ao exigir que os prestadores de serviços de telecomunicações obtenham uma autorização clara e explícita para processar dados sensíveis, incluindo aqueles relacionados com a saúde.

De seguida, através do Artigo 5.º, a diretiva aborda a confidencialidade das comunicações, dispondo que: "*1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no nº 1 do artigo 15.º (...)*" (EU, 2002). Este artigo estabelece uma salvaguarda fundamental para a privacidade dos utilizadores de serviços de comunicações eletrónicas, garantindo que os seus conteúdos não podem ser monitorizados ou divulgados sem o seu consentimento. Esta norma protege tanto as comunicações em tempo real como os dados de tráfego associados às mesmas, impondo uma obrigação adicional clara aos prestadores de serviços de telecomunicações para garantir a segurança das informações transmitidas.

Para além deste, alguns outros artigos abordam questões como o tratamento de dados de tráfego e localização (Artigo 6.º e Artigo 9.º), impondo restrições aos operadores de telecomunicações sobre a recolha e processamento desses dados. No entanto, dado que os

serviços de emergência médica não atuam como fornecedores desse tipo de serviço, a maior relevância desta diretiva é reduzida ao contexto do Artigo 5.º.

4.1.6. Regulamento 2016/679

Amplamente conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD), o Regulamento 2016/679 foi adotado pelo Parlamento Europeu e pelo Conselho da União Europeia a 27 de abril de 2016, tendo entrado em vigor a 25 de maio de 2018. Este regulamento veio substituir a Diretiva 95/46/CE que, embora tenha mantido válidos os seus objetivos e princípios, não conseguiu evitar a fragmentação na aplicação da proteção de dados na União, a insegurança jurídica e a perceção generalizada de que persistiam riscos significativos para a proteção das pessoas singulares (UE, 2016).

A necessidade de um regulamento mais robusto e uniforme surgiu também do crescente avanço tecnológico, da digitalização dos serviços e do aumento exponencial da recolha e tratamento de dados pessoais, exigindo um quadro normativo que assegurasse direitos fundamentais de forma coerente em toda a União Europeia.

Uma das principais inovações deste documento reside na sua aplicabilidade direta em todos os Estados-Membros, sem necessidade de transposição legislativa, garantindo assim uma harmonização mais eficaz da proteção de dados pessoais (UE, 2016). Dada a sua extrema abrangência e consequente relevância para o contexto em estudo, segue-se a análise detalhada dos artigos mais pertinentes, com especial foco nas normas que regulam o tratamento de dados sensíveis, os deveres das entidades responsáveis e as garantias conferidas aos titulares dos dados.

Capítulo I – Disposições gerais

No âmbito de aplicação do regulamento, o Artigo 2.º, n.º 1 especifica os tipos de tratamento de dados pessoais que se encontram abrangidos pela sua legislação: "*O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.*" (UE, 2016). Esta declaração inicial estabelece uma objetiva e essencial delimitação sobre quando o RGPD deve ser aplicado, abrangendo qualquer operação de tratamento de dados pessoais, independentemente de ser realizada através de meios digitais ou físicos, desde que integrada num sistema de organização estruturado.

Ainda nas disposições gerais, o Artigo 4.º estabelece um conjunto de definições fundamentais para a correta interpretação e aplicação do regulamento. Estas definições permitem clarificar os conceitos utilizados ao longo do documento e garantir uma aplicação uniforme em todos os Estados-Membros. No contexto do presente estudo, algumas das alíneas mais relevantes incluem:

- Alínea nº 1 – "*«Dados pessoais», informação relativa a uma pessoa singular (...) que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*" (UE, 2016);
- Alínea nº 2 – "*«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais (...), por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*" (UE, 2016);
- Alínea nº 5 – "*«Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável*" (UE, 2016);
- Alínea nº 8 – "*«Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*" (UE, 2016);
- Alínea nº 11 – "*«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*" (UE, 2016);
- Alínea nº 12 – "*«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a*

divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (UE, 2016);

- Alínea nº 15 – "*«Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde*" (UE, 2016);

Estes conceitos são a base sobre a qual todas as disposições subsequentes do regulamento são construídas. Assim, ao compreender as definições abordadas no Artigo 4.º, torna-se possível interpretar com maior clareza os direitos dos titulares dos dados e as responsabilidades das entidades envolvidas no seu tratamento.

Capítulo II – Princípios

Dando início ao segundo capítulo do regulamento, o Artigo 5.º estabelece os princípios fundamentais que regem o tratamento de dados pessoais, garantindo que este seja realizado de forma justa, transparente e segura.

Assim, o primeiro princípio, previsto na alínea a) do ponto 1, estabelece que os dados pessoais devem ser "*objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*" (UE, 2016). Tal significa que o tratamento deve respeitar uma base legal válida, ser realizado de forma justa e garantir que o titular dos dados é devidamente informado sobre a forma como os seus dados são utilizados.

A alínea b) do mesmo ponto refere o princípio da limitação das finalidades, segundo o qual os dados devem ser "*recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com essas finalidades*" (UE, 2016). Assim, os dados devem ser tratados apenas para os propósitos previamente definidos e comunicados, evitando utilizações abusivas ou inesperadas.

Por sua vez, o princípio da minimização dos dados, estabelecido pela alínea c), determina que os dados devem ser "*adequados, pertinentes e limitados ao que é necessário em relação às finalidades para as quais são tratados*" (UE, 2016). Este princípio impõe que apenas sejam recolhidos os dados essenciais, evitando excessos desnecessários que possam comprometer a privacidade dos titulares. Na prática, a afirmação obriga as entidades responsáveis pelo tratamento a avaliar os dados antes da sua recolha, garantindo que exista sempre uma justificação concreta e proporcional ao objetivo do tratamento.

A alínea d) consagra o princípio da exatidão, estabelecendo que os dados devem ser "*exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora*" (UE, 2016). Tal afirmação significa que a qualidade da informação deve ser garantida, evitando erros que possam prejudicar os titulares dos dados.

No que respeita à conservação dos dados, a alínea e) prevê o princípio da limitação da conservação, estipulando que os dados devem ser "*conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados*" (UE, 2016). Após esse período, os dados devem ser eliminados ou anonimizados, salvo se existir uma obrigação legal que imponha a sua retenção por um período mais longo.

Por fim, a alínea f) estabelece o princípio da integridade e confidencialidade, determinando que os dados devem ser "*tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas*" (UE, 2016). Desta forma, este princípio impõe a adoção de mecanismos de segurança que protejam os dados contra acessos indevidos, fugas de informação ou destruição acidental.

Todos estes princípios constituem a base legal para qualquer tratamento de dados pessoais, garantindo assim um equilíbrio entre a necessidade de utilização dos dados e a proteção dos direitos dos seus titulares.

Relativamente à licitude do tratamento, são descritos nas alínea a) e d) do ponto 1 do Artigo 6.º dois fundamentos distintos, porém complementares, relevantes ao tema em estudo. A primeira alínea baseia-se no princípio de que o tratamento é lícito quando "*O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas*" (UE, 2016). No entanto, este fundamento pode ser insuficiente em determinadas situações, especialmente quando o titular não está em condições de prestar consentimento. Neste contexto, a alínea d) assume especial relevância, permitindo o tratamento dos dados quando "*necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular*" (UE, 2016). Assim, este fundamento aplica-se a todas as circunstâncias em que a proteção da vida ou da integridade física se sobrepõe à

necessidade de obter consentimento, garantindo que o tratamento dos dados possa ocorrer mesmo sem a manifestação de vontade do titular.

Já o Artigo 9.º do regulamento estabelece regras específicas para o tratamento de categorias especiais de dados pessoais, que incluem informações particularmente sensíveis e que, por isso, requerem uma proteção reforçada.

O primeiro ponto deste artigo define a proibição do tratamento de dados pessoais que revelem "a *origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma unívoca, dados relativos à saúde ou dados relativos à vida sexual ou à orientação sexual de uma pessoa*" (UE, 2016). Estes dados, devido à sua natureza sensível, são objeto de um nível de proteção mais elevado, evitando que possam ser utilizados de forma abusiva ou discriminatória.

O ponto 2 estabelece exceções à proibição prevista no ponto anterior, permitindo o tratamento destes dados em determinadas circunstâncias específicas previstas no regulamento, como quando o tratamento for necessário "*c) (...) para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento*", "*h) (...) para fins de medicina preventiva (...), diagnóstico médico, prestação de cuidados ou tratamentos de saúde*", ou "*i) (...) por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*" (UE, 2016). Estas exceções garantem que, em situações críticas, os dados sensíveis possam ser tratados sem violar os princípios fundamentais da proteção de dados.

Já o ponto 3 do mesmo artigo determina ainda que os dados pessoais referidos no ponto 1 podem ser tratados para os fins referidos no nº 2, alínea h), desde que esse tratamento seja realizado "*sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, (...) ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade*" nos termos do direito da União ou do direito nacional (UE, 2016). Esta disposição reforça e garante que, em contextos relacionados com a saúde e a assistência social, o tratamento de dados sensíveis pode ser efetuado, desde que esteja sujeito a rigorosos deveres legais de confidencialidade, assegurando assim a proteção da privacidade dos titulares dos dados.

Capítulo III – Direitos dos titulares dos dados

Relativamente à transparência e às regras para o exercício dos direitos dos titulares dos dados, o nº 1 do Artigo 12.º do RGPD estabelece que o responsável pelo tratamento deve fornecer informações relativas ao tratamento de dados pessoais de forma "*(...) concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças*." (UE, 2016). Além disso, determina que a comunicação pode ser feita por escrito ou por outros meios adequados, incluindo, se for apropriado, por meios eletrónicos. Caso solicitado pelo titular dos dados, as informações podem também ser prestadas oralmente, desde que a identidade do titular seja comprovada por outros meios.

Quanto aos direitos dos titulares dos dados, o Artigo 15.º começa por estabelecer o direito de acesso, permitindo a este "*(...) obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento (...)*" (UE, 2016). Caso os dados sejam tratados, o titular tem o direito de aceder a diversas informações, incluindo "*a) As finalidades do tratamento*", "*b) As categorias de dados pessoais em questão*" e "*c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados (...)*" (UE, 2016).

Além disso, deve ser informado sobre "*d) Se possível, o prazo previsto de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo*" (UE, 2016). Por fim, o mesmo artigo garante também que o titular seja esclarecido sobre "*f) O direito de apresentar reclamação a uma autoridade de controlo*", bem como sobre a origem dos dados que não tenham sido recolhidos junto do mesmo (UE, 2016).

De seguida, o Artigo 16.º consagra ao titular o direito de retificação, permitindo que este obtenha "*(...), sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito.*" (UE, 2016). Além disso, pode exigir que os seus dados "*incompletos sejam completados, incluindo por meio de uma declaração adicional.*" (UE, 2016). Desta forma, este artigo assegura que os titulares dos dados possam corrigir informações incorretas, protegendo a exatidão e integridade dos seus dados pessoais.

O regulamento prevê ainda através do seu Artigo 17.º o direito ao apagamento dos dados pessoais, também conhecido como "direito a ser esquecido". De acordo com o nº 1 deste artigo, o titular dos dados tem o direito de "*(...) obter do responsável pelo tratamento o*

apagamento dos seus dados pessoais, sem demora injustificada (...)", sempre que se aplique uma das seguintes situações: a) os dados deixaram de ser necessários para a finalidade para a qual foram recolhidos, b) o titular retira o consentimento em que se baseava o tratamento, c) o titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes, d) os dados foram tratados ilicitamente, e) devem ser apagados para cumprimento de uma obrigação legal ou f) foram recolhidos no contexto da oferta de serviços da sociedade da informação a crianças (UE, 2016).

No entanto, o artigo prevê exceções em que o direito ao apagamento não se aplica, como por exemplo quando o tratamento dos dados é necessário para exercer a liberdade de expressão e informação, cumprir uma obrigação legal, exercer funções de interesse público, fins de saúde pública, arquivamento de interesse público, investigação científica ou histórica, ou para a declaração, exercício ou defesa de um direito num processo judicial (nº 3) (UE, 2016).

Além destes artigos, o RGPD estabelece também o direito à limitação do tratamento (Artigo 18.º), permitindo ao titular dos dados restringir o uso dos seus dados pessoais em determinadas circunstâncias. De acordo com este artigo, o titular pode solicitar a limitação do tratamento quando "*a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão*", quando "*b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização*", quando "*c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial*", ou quando "*d) O titular dos dados se tiver oposto ao tratamento, até se verificar se os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular*" (UE, 2016).

Este direito garante que os dados não sejam utilizados de forma inadequada enquanto se verifica a sua correção ou a legalidade do seu tratamento, oferecendo ao titular um maior controlo sobre a sua informação pessoal.

Através do Artigo 20.º estabelece-se o direito à portabilidade dos dados, que permite ao titular receber os seus dados pessoais "*(...) num formato estruturado, de uso corrente e de leitura automática (...)*", e transmiti-los a outro responsável pelo tratamento sem

impedimentos. Este direito aplica-se quando o tratamento dos dados se baseia no consentimento do titular e é realizado por meios automatizados (UE, 2016).

O regulamento prevê ainda que, "*2. Ao exercer o seu direito à portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre responsáveis pelo tratamento, sempre que tal seja tecnicamente possível*" (UE, 2016).

Desta forma, o artigo fortalece o controlo dos titulares sobre os seus dados pessoais, facilitando a sua transferência entre serviços e promovendo a interoperabilidade entre diferentes entidades.

Por fim, o Artigo 21.º do RGPD consagra ao titular o direito de oposição, permitindo-lhe contestar o tratamento dos seus dados pessoais em determinadas situações. De acordo com este artigo, o titular pode opor-se "*(...), a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito (...)*", quando esse tratamento se baseia no interesse legítimo do responsável pelo tratamento ou no desempenho de funções de interesse público (UE, 2016). Se o titular exercer este direito, os dados deixam de poder ser tratados, a menos que o responsável demonstre "*razões imperiosas e legítimas para o tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial*" (UE, 2016).

Este último princípio garante que os titulares dos dados possam limitar ou impedir o uso das suas informações pessoais sempre que o seu direito à privacidade se sobreponha aos interesses do responsável pelo tratamento.

Capítulo IV – Responsável pelo tratamento e subcontratante

No âmbito dos deveres do responsável pelo tratamento, o Artigo 24.º estabelece algumas responsabilidades, impondo a este a obrigação de garantir e demonstrar que o tratamento de dados pessoais é realizado em conformidade com o regulamento. Para isso, o responsável deve adotar "*(...) medidas técnicas e organizativas adequadas (...)*" que assegurem e comprovem o cumprimento das normas de proteção de dados, considerando fatores como "*(...) a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoas singulares (...)*" (UE, 2016).

Além disso, quando adequado, o responsável pelo tratamento deve implementar "*(...) políticas adequadas de proteção de dados (...)*", reforçando a necessidade de uma abordagem proativa e preventiva na gestão da privacidade.

Desta forma, este artigo sublinha a responsabilidade ativa das entidades que tratam dados pessoais, exigindo não apenas a conformidade com o RGPD, mas também a capacidade de demonstrar essa conformidade perante as autoridades de controlo.

No mesmo sentido, o artigo seguinte (25.º) estabelece o princípio da proteção de dados desde a conceção e por defeito, exigindo que o responsável pelo tratamento adote medidas que garantam a privacidade e a segurança dos dados pessoais desde o início do seu tratamento. A proteção de dados desde a conceção implica a implementação de "*(...) medidas técnicas e organizativas adequadas (...), destinadas a aplicar com eficácia os princípios da proteção de dados (...)*", assegurando que a privacidade é considerada em todas as fases do processamento de dados. Tal pode incluir medidas como a minimização dos dados, a pseudonimização e restrições de acesso (UE, 2016). Já a proteção de dados por defeito determina que "*(...) apenas sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento (...)*", garantindo que a recolha, armazenamento e utilização dos dados sejam limitados ao estritamente essencial, tanto em termos de volume de dados como de duração do tratamento e acessibilidade (UE, 2016).

Assim, este artigo reforça, uma vez mais, uma abordagem preventiva e proativa, assegurando que os princípios da proteção de dados sejam aplicados desde o primeiro momento em que os dados são tratados.

Uma outra componente de igual relevância para o presente estudo diz respeito ao conceito de subcontratante. Nesse sentido, o Artigo 28.º do documento regula a subcontratação do tratamento de dados, estabelecendo nos termos do nº 1 que o responsável pelo tratamento apenas pode recorrer a subcontratantes que ofereçam "*(...) garantias suficientes de execução de medidas técnicas e organizativas adequadas (...)*" para assegurar a conformidade com o regulamento e a proteção dos direitos dos titulares dos dados (UE, 2016).

É ainda disposto nos termos do nº 3 que o tratamento realizado pelo subcontratante deve ser regido por um "*(...) contrato ou outro ato normativo (...)*", que estipule, entre outros aspetos, que o subcontratante "*(...) trata os dados pessoais apenas mediante instruções*

documentadas do responsável pelo tratamento (...)", que deve garantir a confidencialidade dos dados e que implementará medidas adequadas de segurança (UE, 2016).

Além disso, o subcontratante não pode recorrer a outro subcontratante sem autorização prévia ou específica do responsável pelo tratamento. Caso o faça, deve assegurar que as mesmas obrigações de proteção de dados sejam aplicadas ao novo subcontratante (UE, 2016).

Desta forma, assegura-se que a subcontratação do tratamento de dados decorre de forma controlada e segura, garantindo que os dados pessoais continuam protegidos, mesmo quando são tratados por terceiros.

Para garantir a proteção dos dados, é essencial que sejam implementadas padrões de segurança adequados, conforme estabelecido no Artigo 32.º, onde se impõe ao responsável pelo tratamento e ao subcontratante a adoção de "*(...) medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco (...)*" (UE, 2016). Entre as recomendações incluem-se: "*a) a pseudonimização e cifragem dos dados*", "*b) a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência dos sistemas e dos serviços de tratamento*", "*c) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico*" e "*d) um processo para testar, apreciar e avaliar regularmente a eficácia das medidas*" (UE, 2016).

Além das medidas de segurança previstas pelo artigo anterior, o RGPD também estabelece, para determinadas situações, regras para a designação do cargo de Encarregado da Proteção de Dados, conforme disposto no Artigo 37.º (UE, 2016).

De acordo com o disposto pelo nº 1, um responsável pelo tratamento ou um subcontratante deve, obrigatoriamente, designar um *Data Protection Officer* (DPO) sempre que: "*a) o tratamento for efetuado por uma autoridade ou um organismo público (...)*", quando "*b) as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que (...) exijam um controlo regular e sistemático dos titulares dos dados em grande escala*", ou quando "*c) as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala (...) de dados pessoais relacionados com condenações penais e infrações (...)*" (UE, 2016).

Segundo o nº 5 do mesmo artigo, qualquer encarregado de proteção de dados deverá ser "*(...) designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados (...)*" (UE, 2016).

Relativamente às funções associadas a este cargo, o Artigo 39.º prevê que o DPO deva "*a) informar e aconselhar o responsável pelo tratamento ou o subcontratante (...) a respeito das suas obrigações nos termos do presente regulamento (...)*", bem como "*b) controlar a conformidade (...)*" com o RGPD, assegurando que as políticas e práticas da organização estão alinhadas com as exigências legais (UE, 2016). Além disso, deve "*c) prestar aconselhamento (...)*", "*d) cooperar com a autoridade de controlo*" e servir de "*e) ponto de contacto (...)*" para com esta (UE, 2016).

Capítulo VIII – Vias de recurso, responsabilidade e sanções

De forma a assegurar o cumprimento por parte de todos os Estados-Membros, o regulamento prevê um regime sancionatório rigoroso. Esse regime é estabelecido, numa primeira fase, pelo Artigo 83.º, que define as regras para a aplicação de coimas administrativas, determinando os critérios e os montantes máximos das sanções em caso de incumprimento (UE, 2016).

O artigo inicia dispondo que as autoridades de controlo devem garantir que as coimas são "*(...) efetivas, proporcionadas e dissuasoras (...)*", tendo em conta diversos fatores listados pelo nº 2, como "*a) a natureza, a gravidade e a duração da infração (...)*", "*b) o caráter intencional ou negligente da infração*", "*d) o grau de responsabilidade do responsável pelo tratamento ou do subcontratante (...)*", entre outros fatores agravantes ou atenuantes aplicáveis às circunstâncias do caso (UE, 2016).

De seguida, o regulamento prevê dois níveis de sanções: as infrações menos graves - como violações das obrigações do responsável pelo tratamento, do subcontratante ou do organismo de supervisão - que podem ser punidas com coimas até 10 milhões de euros ou 2% do volume de negócios anual global, consoante o valor mais elevado; e as infrações mais graves - como violações dos princípios básicos do tratamento de dados, dos direitos dos titulares ou da transferência ilegal de dados para países terceiros - que podem resultar em coimas até 20 milhões de euros ou 4% do volume de negócios anual global, também consoante o valor mais elevado (UE, 2016).

Capítulo IX – Disposições relativas a situações específicas de tratamento

Por fim, importa ainda referir o Artigo 90.º, que regula as obrigações de sigilo profissional e confidencialidade no tratamento de dados pessoais (UE, 2016). Neste âmbito, o artigo prevê que os Estados-Membros possam "*adotar regras específicas para estabelecer os poderes das autoridades de controlo (...) relativamente a responsáveis pelo tratamento ou subcontratantes sujeitos (...) a uma obrigação de sigilo profissional ou a outras obrigações de sigilo equivalentes, caso tal seja necessário e proporcionado para conciliar o direito à proteção de dados pessoais com a obrigação de sigilo.*" (UE, 2016).

Desta forma, o regulamento reconhece que, em alguns casos, é necessário assegurar que os responsáveis pelo tratamento e os subcontratantes respeitem normas de confidencialidade, especialmente quando o tratamento envolve trabalhadores sujeitos ao sigilo profissional, como médicos ou outros prestadores de serviços que lidam com informações sensíveis.

Através destes e de outros artigos, o RGPD reforçou significativamente os direitos dos titulares dos dados, impôs obrigações mais rigorosas às entidades responsáveis pelo tratamento e introduziu sanções severas para violações das suas disposições. Também a introdução de conceitos inovadores, como a responsabilidade ativa, a minimização dos dados e a transparência no tratamento, tornaram-no num dos regulamentos mais abrangentes e influentes no domínio da privacidade e segurança da informação. Atualmente, o seu impacto ultrapassa as fronteiras da União Europeia, servindo de referência para outras legislações e reforçando a necessidade de uma cultura de proteção de dados mais robusta e centrada na defesa dos direitos fundamentais dos cidadãos.

4.1.7. Proposta do Espaço Europeu de Dados de Saúde

Atualmente, apesar da proteção conferida pelo RGPD, a aplicação e interpretação desiguais das suas disposições nos diferentes Estados-Membros têm gerado incertezas jurídicas, tanto a nível nacional como transfronteiriço. Além disso, as pessoas singulares têm sentido dificuldade em exercer os seus direitos sobre os seus dados de saúde eletrónicos, incluindo no que diz respeito ao acesso aos mesmos e à sua transmissão a nível nacional e transfronteiras (UE, 2022).

Assim, a 3 de maio de 2022, a CE apresentou um dos primeiros e mais ambiciosos espaços comuns europeus de dados através da proposta do Regulamento do Espaço Europeu de Dados de Saúde, como parte da Estratégia Europeia para os Dados (UE, 2022).

Este novo regulamento surgiu, portanto, com o objetivo de criar um quadro jurídico harmonizado para a partilha e proteção dos dados de saúde eletrónicos dentro da UE, garantindo que as pessoas singulares têm um maior controlo sobre as suas informações de saúde e que esses dados podem ser utilizados de forma segura e eficiente para fins secundários, como investigação, inovação e formulação de políticas públicas (UE, 2022). Além de melhorar a acessibilidade e a portabilidade dos dados para os cidadãos, a proposta visou também criar um mercado único para produtos e serviços digitais na área da saúde, promovendo a interoperabilidade e eficiência dos sistemas de saúde na UE (UE, 2022).

Assim, em março de 2024, o Parlamento Europeu e o Conselho da UE chegaram a um acordo provisório sobre o texto do regulamento, avançando para a sua adoção formal. Finalmente, o documento foi adotado a 21 de janeiro de 2025, marcando um passo essencial para a digitalização segura do setor (Conselho União Europeia, 2025).

É ainda de notar que a estrutura da proposta assenta em diversas legislações europeias relevantes, como o RGPD, o Regulamento (UE) 2017/745 relativo aos dispositivos médicos, a proposta de Regulamento Inteligência Artificial, a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação, entre outros (UE, 2022).

Além dessas legislações, o Espaço Europeu de Dados de Saúde estabelece o seu próprio âmbito de aplicação, determinando as entidades e os contextos em que as suas disposições são aplicáveis. Nesse sentido, o n.º 3 do Artigo 1.º define o âmbito de aplicação do regulamento, especificando que o mesmo se aplica "*a) Aos fabricantes e fornecedores de sistemas de RSE e aplicações de bem-estar colocados no mercado e colocados em serviço na União, bem como aos utilizadores desses produtos*" e também "*b) Aos responsáveis pelo tratamento e subcontratantes estabelecidos na União que tratam dados de saúde eletrónicos de cidadãos da União (...)*" (UE, 2022). Ou seja, segundo este artigo, qualquer entidade dentro da UE que processe dados de saúde eletrónicos, como hospitais, clínicas, serviços de emergência e entidades públicas, deve cumprir o regulamento.

O documento abrange ainda "*c) os responsáveis pelo tratamento e subcontratantes estabelecidos num país terceiro que tenham sido ligados a A minha saúde @ UE (MyHealth@EU) ou sejam interoperáveis com esta infraestrutura (...)*" e "*d) os utilizadores de dados a quem são disponibilizados dados de saúde eletrónicos por detentores de dados na União*" (UE, 2022)., assegurando que qualquer entidade ou profissional que tenha acesso a dados de saúde eletrónicos cumpra as regras do regulamento.

No n.º 2 do Artigo 2.º, o documento apresenta um conjunto de definições essenciais para a aplicação do regulamento. Entre elas, destacam-se algumas alíneas que clarificam conceitos fundamentais no contexto da utilização e proteção dos dados de saúde eletrónicos:

- Alínea a) – "*«Dados de saúde eletrónicos pessoais», os dados relativos à saúde e os dados genéticos na aceção do Regulamento (UE) 2016/679, bem como os dados referentes a determinantes da saúde ou os dados tratados no âmbito da prestação de serviços de saúde, que são tratados em formato eletrónico*" (UE, 2022);
- Alínea d) – "*«Utilização primária de dados de saúde eletrónicos», o tratamento de dados de saúde eletrónicos pessoais para a prestação de serviços de saúde a fim de avaliar, manter ou restabelecer o estado de saúde da pessoa singular a quem esses dados dizem respeito (...)*" (UE, 2022);
- Alínea m) – "*«RSE» (registo de saúde eletrónico), um conjunto de dados de saúde eletrónicos relativos a uma pessoa singular e recolhidos no sistema de saúde, tratados para fins de cuidados de saúde*" (UE, 2022);
- Alínea n) – "*«Sistema de RSE» (sistema de registos de saúde eletrónicos), qualquer dispositivo ou software destinado pelo fabricante a ser utilizado para conservação, intermediação, importação, exportação, conversão, edição ou visualização de registos de saúde eletrónicos*" (UE, 2022);
- Alínea t) – "*«A minha saúde @ UE (MyHealth@EU)», a infraestrutura transfronteiriça para a utilização primária de dados de saúde eletrónicos constituída pela combinação dos pontos de contacto nacionais para a saúde digital e a plataforma central para a saúde digital*" (UE, 2022);

No âmbito dos direitos das pessoas singulares em relação à utilização dos seus dados de saúde eletrónicos, o Artigo 3.º do EEDS estabelece garantias essenciais relacionadas com o acesso, transparência e eventuais restrições justificadas (UE, 2022).

Nesse sentido, o nº 1 deste artigo garante que "*As pessoas singulares têm o direito de aceder imediatamente, a título gratuito e de forma facilmente legível, consolidada e acessível aos seus dados de saúde eletrónicos pessoais tratados no contexto da utilização primária de dados de saúde eletrónicos*" (UE, 2022). Esta primeira disposição assegura que os cidadãos podem consultar os seus registos de saúde eletrónicos sem custos e sem barreiras, permitindo-lhes gerir dados essenciais para a sua saúde de forma autónoma e informada.

De seguida, o n.º 3 introduz uma exceção a este direito, estabelecendo que, "*Em conformidade com o artigo 23.º do Regulamento (UE) 2016/679, os Estados-Membros podem limitar o alcance deste direito sempre que seja necessário para a proteção da pessoa singular, por razões de segurança dos doentes e de ética, diferindo o acesso aos seus dados de saúde eletrónicos pessoais durante um período limitado, até que um profissional de saúde possa transmitir e explicar devidamente à pessoa singular as informações suscetíveis de ter um impacto significativo na sua saúde*" (UE, 2022). Esta limitação tem como principal objetivo proteger pacientes de informações que possam gerar um impacto psicológico negativo ou necessitem de mediação médica para serem compreendidas corretamente, evitando possíveis reações adversas ou decisões precipitadas por parte dos titulares.

Por fim, é ainda de notar o n.º 10 que dispõe que "*As pessoas singulares têm o direito de obter informações sobre os prestadores de cuidados de saúde e os profissionais de saúde que acederam aos seus dados de saúde eletrónicos no contexto dos cuidados de saúde. As informações devem ser prestadas de forma imediata e gratuita através de serviços de acesso a dados de saúde eletrónicos*" (UE, 2022). Através desta declaração reforça-se a transparência no tratamento de dados, garantindo que os titulares possam verificar quem acedeu às suas informações de saúde, reduzindo o risco de incidentes no tratamento dos dados.

Além de garantir os direitos das pessoas singulares sobre os seus dados de saúde eletrónicos, a proposta de regulamento estabelece também regras específicas para o acesso dos profissionais de saúde a essas informações, conforme definido no Artigo 4.º.

O n.º 1 deste artigo prevê que os profissionais de saúde devem "*a) Ter acesso aos dados de saúde eletrónicos das pessoas singulares que tratam, independentemente do Estado-Membro de afiliação e do Estado-Membro de tratamento*" (UE, 2022). Esta medida assegura que os dados clínicos das vítimas e pacientes possam ser consultados por profissionais de saúde em toda a União Europeia, facilitando o atendimento em contexto transfronteiriço. Além disso, o artigo determina que os profissionais devem "*b) Assegurar que os dados de saúde eletrónicos pessoais das pessoas singulares que tratam sejam atualizados com informações relativas aos serviços de saúde prestados*" (UE, 2022), garantindo a fiabilidade dos registos clínicos.

O quarto ponto introduz ainda algumas salvaguardas relacionadas com o direito dos titulares a restringirem o acesso aos seus dados, através da disposição: "*Se o acesso aos*

dados de saúde eletrónicos tiver sido restringido pela pessoa singular, o prestador de cuidados de saúde ou os profissionais de saúde não podem ser informados do conteúdo dos dados de saúde eletrónicos sem autorização prévia da pessoa singular (...)" (UE, 2022). No entanto, tal como também explorado pelo RGPD, esta proposta prevê uma exceção para situações em que seja necessário garantir a proteção dos interesses vitais do titular dos dados ou de outra pessoa singular, permitindo, nesses casos, que o prestador de cuidados de saúde aceda aos dados restringidos. Após esse acesso, "*(...) o prestador de cuidados de saúde ou o profissional de saúde deve informar o detentor dos dados e a pessoa singular em causa ou os seus tutores de que foi concedido acesso aos dados de saúde eletrónicos*" (UE, 2022).

Para garantir a acessibilidade e partilha eficiente de dados de saúde eletrónicos, o regulamento estabelece categorias prioritárias de informação médica essenciais para a prestação de cuidados.

Nesse sentido, o Artigo 5.º define que "*(...) os Estados-Membros devem assegurar o acesso e o intercâmbio de dados de saúde eletrónicos pessoais para utilização primária que se enquadrem total ou parcialmente (...)*" em categorias específicas (UE, 2022). Entre estas incluem-se "*a) Resumos de saúde dos doentes; b) Receitas eletrónicas; c) Dispensas eletrónicas; d) Imagiologia e relatórios imagiológicos; e) Resultados laboratoriais; e f) Relatórios de alta*" (UE, 2022).

Este artigo assume maior relevância tendo em conta o n.º 3 do artigo anterior que define que os Estados-Membros devem assegurar que os profissionais de saúde tenham "*(...) acesso, pelo menos, às categorias prioritárias de dados de saúde eletrónicos a que se refere o artigo 5.º, através de serviços de acesso dos profissionais de saúde*" (UE, 2022). Além disso, os profissionais que possuam "*(...) meios de identificação eletrónica reconhecidos têm o direito de utilizar esses serviços de acesso dos profissionais de saúde a título gratuito*" (UE, 2022).

Desta forma, as disposições reforçam a interoperabilidade dos sistemas de saúde, permitindo que os profissionais disponham das informações essenciais para a prestação de cuidados, sem comprometer a segurança e a privacidade dos dados.

Por fim, a proposta do EEDS termina o seu capítulo segundo com dois artigos, 12.º e 13.º, que regulam a infraestrutura "*A minha saúde @ UE (MyHealth@EU)*", essencial na troca transfronteiriça de dados de saúde eletrónicos entre os Estados-Membros.

Através do n.º 1 do primeiro artigo estabelece-se que "*Cabe à Comissão criar uma plataforma central para a saúde digital, a fim de prestar serviços destinados a apoiar e facilitar o intercâmbio de dados de saúde eletrónicos entre os pontos de contacto nacionais para a saúde digital dos Estados-Membros.*" (UE, 2022).

Além disso, o ponto n.º 2 determina que "*Cada Estado-Membro deve designar um ponto de contacto nacional para a saúde digital (...)*", responsável por assegurar a ligação entre todos os pontos de contacto nacionais e a plataforma central para a saúde digital (UE, 2022). Esta estrutura permite que os dados dos pacientes sejam partilhados entre diferentes países da UE, garantindo que os profissionais de saúde possam aceder a informações médicas essenciais sempre que necessário.

Para garantir a segurança e interoperabilidade do sistema, o n.º 4 do mesmo artigo prevê que "*A Comissão adota, por meio de atos de execução, as medidas necessárias para o desenvolvimento técnico de A minha saúde @ UE (MyHealth@EU), as regras pormenorizadas relativas à segurança, à confidencialidade e à proteção dos dados de saúde eletrónicos (...)*" (UE, 2022). Desta forma, pretende-se estabelecer normas rigorosas para proteção da privacidade dos dados eletrónicos e definir as condições para a adesão e manutenção da ligação à plataforma.

Por fim, é estipulado pelos termos do n.º 5 que "*Os Estados-Membros devem assegurar a ligação de todos os prestadores de cuidados de saúde aos respetivos pontos de contacto nacionais para a saúde digital e assegurar que os prestadores de cuidados de saúde ligados possam proceder ao intercâmbio bidirecional de dados de saúde eletrónicos com o ponto de contacto nacional para a saúde digital.*" (UE, 2022). Tal disposição significa que hospitais, clínicas e serviços de emergência devem estar integrados na infraestrutura, permitindo um fluxo contínuo de informação entre diferentes entidades, independentemente do país onde operam.

Em suma, embora o EEDS ainda não esteja plenamente implementado em todos os Estados-Membros, devido à sua recente data de adoção, representa um avanço significativo na digitalização e interoperabilidade dos sistemas de saúde na União Europeia. Ao estabelecer regras claras para o acesso, partilha e proteção dos dados de saúde eletrónicos, o regulamento visa melhorar a continuidade dos cuidados, reforçar os direitos dos titulares dos dados e garantir a segurança da informação médica. A introdução da infraestrutura MyHealth@EU e a definição de categorias prioritárias de dados reforçam a necessidade de

um ambiente seguro e eficiente para o intercâmbio de informações de saúde, promovendo maior cooperação entre os sistemas nacionais de saúde e facilitando a prestação de cuidados, especialmente em contextos transfronteiriços e de emergência.

4.1.8. Diretiva 2022/2555

Também conhecida como SRI/NIS 2, a Diretiva (UE) 2022/2555 foi adotada pela União Europeia a 14 de dezembro de 2022 e publicada no Jornal Oficial da UE a 27 de dezembro de 2022. Este novo documento veio substituir a Diretiva (UE) 2016/1148 (Diretiva SRI/NIS), que foi a primeira legislação da UE dedicada à segurança das redes e da informação (UE, 2022).

Uma das principais razões que motivaram à revisão da diretiva centra-se no aumento da frequência e sofisticação dos ciberataques, que demonstraram a necessidade de um quadro regulatório mais robusto e harmonizado entre os Estados-Membros. Além disso, o relatório de avaliação da aplicação da Diretiva NIS original, publicado pela Comissão Europeia em 2020, revelou disparidades significativas na implementação das regras de Cibersegurança nos diferentes países, bem como lacunas na proteção de infraestruturas críticas e serviços essenciais (CE, 2020).

Nesse sentido, a Diretiva NIS 2 foi concebida para reforçar a resiliência das infraestruturas digitais e dos setores críticos, impondo regras mais rigorosas de gestão de riscos e resposta a incidentes, alargando o número de setores e entidades abrangidas e promovendo maior cooperação entre os Estados-Membros. A transposição para a legislação nacional dos Estados-Membros ocorreu até 17 de outubro de 2024, altura em que a diretiva entrou plenamente em vigor em toda a União Europeia (UE, 2022).

Embora o documento abranja um vasto conjunto de disposições sobre Cibersegurança, a maioria dos seus artigos é direcionada para equipas de Resposta a Incidentes de Segurança Informática (CSIRT), mecanismos de cooperação e supervisão. No entanto, alguns artigos são particularmente relevantes para este estudo, nomeadamente aqueles que estabelecem o âmbito de aplicação, as obrigações das entidades essenciais e as medidas de gestão de riscos.

Assim, o Artigo 1.º começa por definir o objeto da diretiva, estabelecendo que esta visa "*(...) garantir um elevado nível comum de cibersegurança em toda a União (...)*", reforçando a resiliência dos setores essenciais e a resposta a incidentes de segurança (UE, 2022). Para isso, o ponto 2 do mesmo artigo estabelece diversos padrões como "*a) A*

obrigação de os Estados-Membros adotarem estratégias nacionais de cibersegurança (…)", "*b) Medidas de gestão dos riscos e obrigações de notificação (…)*", "*c) Regras e obrigações em matéria de partilha de informações (…)*", e ainda "*d) Obrigações em matéria de supervisão e execução (…)*" (UE, 2022).

Para concretizar esses objetivos, a diretiva define no Artigo 2.º o seu âmbito de aplicação, especificando as entidades e setores abrangidos pelas suas disposições.

Nesse sentido, o primeiro ponto do artigo determina que a diretiva se aplica a "*(…) entidades públicas ou privadas de um dos tipos referidos no anexo I ou II, que sejam consideradas médias empresas (…), e que prestem os seus serviços ou exerçam as suas atividades na União.*" (UE, 2022). Entre os setores definidos pelo anexo I, inclui-se a saúde, nomeadamente entidades prestadoras de cuidados de saúde, a energia, os transportes, a administração pública, o espaço, entre outros (UE, 2022).

No n.º 2 a diretiva expande a sua aplicação para entidades que, independentemente da sua dimensão, desempenhem um papel fundamental em setores críticos. Entre os critérios que justificam essa inclusão, destaca-se a alínea c), que prevê que a NIS 2 também se aplica às entidades onde "*uma perturbação do serviço prestado (…) possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública*" (UE, 2022).

O número seguinte reforça essa abordagem ao determinar que a diretiva também se aplica "*(…) às entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557.*", que regula a resiliência das infraestruturas essenciais, independentemente da dimensão que tenham (UE, 2022).

Por fim, o n.º 6 e o n.º 7 do mesmo artigo clarificam que a diretiva não se aplica a entidades que desempenham funções de segurança nacional, defesa ou aplicação da lei, mantendo estas áreas sob legislação específica dos Estados-Membros (UE, 2022).

Desta forma, o Artigo 2.º estabelece rigorosos critérios para determinar quais entidades estão sujeitas à NIS 2, assegurando que setores críticos e entidades com impacto significativo na sociedade adotem medidas de segurança rigorosas, independentemente da sua dimensão.

No sentido de estabelecer critérios para determinar o nível de obrigações de Cibersegurança que cada organização deve cumprir, o Artigo 3.º da Diretiva define as entidades entre essenciais e importantes.

Dessa forma, o ponto n.º 1 classifica como essenciais "*Entidades de um dos tipos referidos no anexo I que excedam os limiares para as médias empresas (...)*", "*Prestadores de serviços de confiança qualificados e registos de nomes de domínio de topo, bem como prestadores de serviços de DNS (...)*", "*Fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público (...)*", "*Entidades da administração pública (...)*" e "*Entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557*" (UE, 2022).

Já o n.º 2 estabelece que as entidades importantes são aquelas que pertencem aos setores listados no Anexo I ou II, mas que não se qualificam como essenciais. Assim, estão sujeitas a obrigações, embora com um nível de supervisão menos rigoroso (UE, 2022).

A distinção entre estes dois grupos torna-se fundamental, uma vez que determina o grau de exigência na implementação de medidas de segurança e a intensidade da supervisão pelas autoridades nacionais.

Através do Artigo 6.º, a Diretiva apresenta, como habitual, um conjunto de definições fundamentais, algumas das quais particularmente relevantes para a compreensão e aplicação das disposições abordadas por este subcapítulo:

- Alínea 4) – "*«Estratégia nacional de cibersegurança», um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos no domínio da cibersegurança e define a governação com vista à sua consecução no Estado-Membro em causa*" (UE, 2022);
- Alínea 6) – "*«Incidente», um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes*" (UE, 2022);
- Alínea 8) – "*«Tratamento de incidentes», todas as ações e procedimentos que visam a prevenção, a deteção, a análise, a contenção ou a resposta a um incidente e a recuperação de um incidente*" (UE, 2022);
- Alínea 9) – "*«Risco», a possível perda ou perturbação causada por um incidente, expressa como uma combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente*" (UE, 2022);
- Alínea 35) – "*«Entidade da administração pública», uma entidade, reconhecida como tal num Estado-Membro, nos termos do direito nacional, não incluindo o*

> *poder judicial, os parlamentos ou os bancos centrais, que cumpra os seguintes critérios: a) Foi criada para satisfazer necessidades de interesse geral e não tem carácter industrial ou comercial*" (UE, 2022).

Após estabelecer estes conceitos, o documento avança para a regulamentação das entidades abrangidas e dos seus deveres, incluindo a implementação de medidas de gestão de riscos de Cibersegurança.

Nesse sentido, o Artigo 21.º impõe através do seu n.º 1 que estas entidades adotem "*(...) medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança dos sistemas de rede e informação que utilizam nas suas operações ou na prestação dos seus serviços (...)*" (UE, 2022). Essas medidas devem ser proporcionais ao nível de risco, tendo em conta os progressos tecnológicos, normas internacionais e os custos de implementação. Além disso, a avaliação da proporcionalidade das medidas deve considerar fatores como a dimensão da entidade, o grau de exposição a riscos e o impacto social e económico de eventuais incidentes (UE, 2022).

De forma complementar, o ponto n.º 2 do mesmo artigo determina ainda que as medidas adotadas devem basear-se numa abordagem abrangente de todos os riscos, protegendo sistemas de rede e informação, bem como o seu ambiente físico contra incidentes. Entre os requisitos obrigatórios, as entidades devem assegurar a implementação de todas as seguintes medidas (UE, 2022):

- "*a) Políticas de análise dos riscos e de segurança dos sistemas de informação*";
- "*b) Tratamento de incidentes*";
- "*c) Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises*";
- "*d) Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos*";
- "*e) Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades*";
- "*f) Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de Cibersegurança*";
- "*g) Práticas básicas de ciber-higiene e formação em Cibersegurança*";

- "*h) Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem*";
- "*i) Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos*";
- "*j) Utilização de soluções de autenticação multifatores ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, se for caso disso*".

Desta forma, as disposições garantem que as infraestruturas essenciais, incluindo os serviços de saúde e emergência, adotem medidas eficazes de Cibersegurança, protegendo a privacidade dos dados dos titulares e garantindo a continuidade das operações críticas.

Para assegurar uma resposta eficaz aos incidentes, a diretiva impõe também algumas exigências que garantem uma comunicação rápida e coordenada com as autoridades competentes.

Como tal, o Artigo 23.º estabelece obrigações de notificação de incidentes para as entidades abrangidas, nomeadamente através do n.º 1 que determina que estas devem notificar, sem demora injustificada, "*(...) qualquer incidente que tenha um impacto significativo na prestação dos seus serviços (...)*" às autoridades competentes ou às equipas CSIRT (UE, 2022).

Nos termos do n.º 4 define-se ainda que os Estados-Membros devem garantir que as entidades abrangidas apresentem notificações estruturadas em diferentes fases. Nesse sentido, um alerta rápido deve ser enviado dentro de 24 horas após a deteção do incidente, indicando se há suspeitas de atividade ilícita ou impacto transfronteiriço. Já no prazo máximo de 72 horas, deve ser enviada uma notificação de incidente, com uma avaliação inicial da gravidade e impacto. Por fim, no prazo de um mês, as entidades devem apresentar um relatório final, detalhando a causa, impacto e medidas adotadas (UE, 2022).

Assim, estas regras permitem garantir transparência, comunicação rápida e mitigação eficaz de qualquer incidente, minimizando o impacto sobre infraestruturas críticas e sobre os dados sensíveis.

Por fim, o Artigo 36.º da NIS 2 determina que os Estados-Membros devem definir e implementar "*(...) regras relativas às sanções aplicáveis em caso de violação das disposições nacionais adotadas nos termos da presente diretiva e tomam todas as medidas*

necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas" (UE, 2022). Além disso, a diretiva prevê ainda que "*Os Estados-Membros notificam a Comissão, até 17 de janeiro de 2025, dessas regras e dessas medidas e também, sem demora, de qualquer alteração ulterior*" (UE, 2022).

Desta forma, o artigo assegura que as entidades que não cumpram as exigências da NIS 2 enfrentem consequências adequadas, promovendo uma aplicação uniforme e rigorosa da diretiva em toda a União Europeia.

Em suma, a Diretiva NIS 2 representa mais um avanço significativo na regulamentação da Cibersegurança na UE, reforçando a resiliência das infraestruturas críticas e estabelecendo obrigações mais rigorosas para a proteção dos sistemas de informação. Apesar de ser um documento bastante focado em entidades como as CSIRT e as autoridades competentes, o seu impacto estende-se a todos os setores essenciais, incluindo a saúde, onde constitui mais uma camada de proteção extra para os dados de saúde e para a continuidade dos serviços de emergência.

No entanto, sendo uma regulamentação recente, a sua implementação prática ainda levará tempo, exigindo adaptações por parte dos Estados-Membros e das entidades abrangidas para garantir a sua aplicação eficaz no contexto real.

Sob forma de conclusão do subcapítulo, o enquadramento normativo europeu reflete o compromisso da União Europeia em reforçar a proteção dos dados pessoais e a Cibersegurança, garantindo a resiliência dos serviços essenciais e a confiança no ambiente digital. Embora a Declaração Universal dos Direitos Humanos, as Convenções e a Carta dos Direitos Fundamentais sejam relativamente limitadas e vagas no que diz respeito ao tratamento e proteção de dados e à segurança da informação, foram fundamentais para estabelecer a base jurídica e os princípios que orientaram a criação de regulamentações mais robustas e específicas.

Nesse contexto, o RGPD, o EEDS e a Diretiva NIS 2 representam uma evolução significativa, assegurando uma maior proteção dos dados e da privacidade dos titulares. Com estas regulamentações, a UE visa harmonizar as práticas entre os Estados-Membros, mitigar riscos e responder eficazmente a incidentes e ameaças, promovendo um ecossistema de dados seguro e interoperável, essencial para setores críticos como o da saúde e da emergência pré-hospitalar.

4.2. Direito nacional

A legislação nacional sobre proteção de dados pessoais e de saúde surge da necessidade de garantir a segurança da informação, a confidencialidade e a privacidade dos titulares, alinhando-se com os princípios estabelecidos pelo direito europeu, mas também considerando as especificidades e desafios próprios do contexto português. Com o crescente avanço tecnológico e a digitalização massiva dos serviços, tornou-se essencial definir regras claras e eficazes para o tratamento dos dados, especialmente aqueles relacionados a setores críticos como a saúde.

Assim, ao longo dos últimos anos, a legislação nacional tem vindo a evoluir e adaptar-se às normas europeias, com a transposição de diretivas e a implementação de regulamentações específicas que garantem um equilíbrio entre inovação tecnológica e proteção da privacidade. Paralelamente, as entidades reguladoras assumem um papel fundamental na fiscalização, regulamentação e orientação das práticas de tratamento de dados, promovendo um ambiente mais seguro, transparente e confiável para profissionais e cidadãos.

É nesse contexto que, neste subcapítulo, será analisado o quadro normativo nacional, explorando os diplomas legais mais relevantes e a forma como estes estruturam a proteção de dados em Portugal, com particular foco no setor da saúde e nos serviços de emergência. Essa abordagem permitirá compreender de forma mais aprofundada como as normas nacionais se articulam com o direito europeu e quais os mecanismos aplicados para assegurar a conformidade e a segurança no tratamento de informações sensíveis.

4.2.1. Lei nº 41/2004, de 18 de agosto

Promulgada no início do século e ainda em vigor, a Lei n.º 41/2004, de 18 de agosto, estabelece as regras para a proteção da privacidade nas comunicações eletrónicas, regulando o tratamento de dados pessoais, a segurança das redes e a confidencialidade das comunicações. Sendo uma transposição da Diretiva 2002/58/CE, esta lei segue os princípios europeus já definidos, mas introduz algumas adaptações ao contexto nacional (AR, 2004). Nesse sentido, a sua análise servirá apenas para destacar as alterações ou adições mais relevantes face à diretiva original.

Uma das primeiras e mais relevantes novidades surge no Artigo 4.º, n.º 4, que estabelece que "*São autorizadas as gravações de comunicações de e para serviços públicos destinados*

a prover situações de emergência de qualquer natureza" (AR, 2004). Desta forma, esta disposição, ausente na diretiva transposta, introduz uma exceção ao princípio da inviolabilidade das comunicações, permitindo a gravação de chamadas para serviços públicos de emergência.

O tratamento de dados de localização para fins de resposta a emergências é outra das novas alterações abordadas pelo Artigo 7.º, n.º 2. Através da disposição "*É permitido o registo, tratamento e transmissão de dados de localização às organizações com competência legal para receber chamadas de emergência para efeitos de resposta a essas chamadas*", esta norma permite que as entidades de emergência e socorro tenham acesso a essas informações, garantindo um apoio mais rápido e eficaz na assistência às vítimas (AR, 2004).

A presente lei estabelece ainda no nº 3 do Artigo 10.º que, as empresas que oferecem serviços de comunicações eletrónicas, mencionadas no n.º 1 do mesmo artigo, têm a obrigação de "*(...) anular, numa base linha a linha, a eliminação da apresentação da linha chamadora (...)*" sempre que a chamada seja efetuada para um serviço de emergência (AR, 2004). Desta forma, é garantida a impossibilidade de ocultação do número de telefone do contactante, permitindo que as linhas de socorro adquiram essa informação.

Relativamente à forma como os clientes das empresas de telecomunicações fornecem o seu consentimento para os fins previstos pelos artigos anteriormente explorados, a alínea b) do nº 5 do Artigo 7.º, determina que essas informações podem ser transmitida através de cláusulas nos contratos celebrados ou por comunicação expressa nos contratos já existentes, garantindo que todos os utilizadores estejam cientes do tratamento realizado aos seus dados de localização (AR, 2004). Por fim, o ponto nº 6 do mesmo artigo define ainda que a utilização desses dados deve ser restringida ao fim para que foi concedida (AR, 2004).

As últimas alterações de relevância encontradas aquando da comparação da lei com a diretiva que transpõe dizem respeito ao regime sancionatório, que estabelece coimas distintas consoante a gravidade das infrações. Estas situações estão previstas pelo Artigo 14.º que prevê penalizações para situações como a violação do dever de confidencialidade e o armazenamento inadequado de dados de tráfego e localização. Além disso, distingue as contraordenações praticadas por pessoas singulares e coletivas, aplicando sanções mais severas às entidades responsáveis pelo tratamento de dados. Por último, o ponto nº 4 prevê ainda que a tentativa e a negligência sejam puníveis, reforçando a necessidade de cumprimento rigoroso das normas.

Em conclusão, a análise das modificações introduzidas na transposição da Diretiva 2002/58/CE para o direito nacional evidencia a atenção dada ao tratamento das chamadas de emergência, com a introdução de disposições específicas que permitem a gravação das comunicações, o acesso a dados de localização e a anulação da ocultação da linha chamadora. Estas adições reforçam a importância da eficiência e prontidão na resposta a situações críticas, garantindo que as entidades de emergência disponham das ferramentas necessárias para atuar de forma mais rápida e precisa, sem comprometer a privacidade das vítimas fora deste contexto.

4.2.2. Lei nº 12/2005, de 26 de janeiro

O regime jurídico dos dados de saúde em Portugal é, em parte, definido pela Lei n.º 12/2005, de 26 de janeiro, que regula o tratamento, acesso e proteção da informação genética e pessoal de saúde dos cidadãos. Esta legislação estabelece os princípios fundamentais para a gestão e utilização desses dados, garantindo que o seu tratamento respeita os direitos de privacidade, confidencialidade e segurança. Além disso, determina quem pode aceder às informações, em que condições esse acesso pode ocorrer e quais as obrigações das entidades responsáveis pelo seu tratamento (AR, 2005).

Embora esta lei tenha um alcance geral sobre os dados clínicos, grande parte dos seus artigos são especificamente direcionados para áreas mais específicas, como o tratamento de dados genéticos, a sua utilização para fins de seguros, a investigação científica, a conservação de material biológico, o património genético humano e a criação e gestão de bancos de ADN (AR, 2005). Estes temas refletem a necessidade de regular a recolha e o uso de informação sensível, garantindo que é utilizada de forma ética e em conformidade com os direitos dos titulares.

No entanto, alguns artigos iniciais deste documento abordam as informações de saúde de forma mais ampla, estabelecendo princípios gerais sobre o tratamento e acesso a dados deste tipo, que podem ser relevantes para o contexto do presente estudo.

Nesse sentido, o Artigo 2.º da presente lei começa por definir o conceito de informação de saúde, estabelecendo um âmbito abrangente para os dados protegidos por esta legislação. De acordo com esta disposição, a informação de saúde "*(...) abrange todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar*" (AR, 2005).

A relevância deste artigo evidencia-se pelo facto de reconhecer a sensibilidade dos dados de saúde, incluindo não apenas as condições médicas atuais, mas também informações preditivas sobre a saúde futura do titular. Além disso, ao incluir a história clínica e familiar, a lei reconhece a importância dos antecedentes médicos, que podem ser determinantes para diagnósticos, tratamentos e investigações científicas.

No seguimento do documento, são estabelecidos princípios essenciais sobre a posse e o acesso a essa informação, garantindo direitos fundamentais aos titulares e delimitando as responsabilidades das entidades que a tratam. Assim, o Artigo 3.º começa por refletir essa preocupação ao definir no seu nº 1 que "*A informação de saúde, incluindo os dados clínicos registados, (...) é propriedade da pessoa, sendo as unidades do sistema de saúde os depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados (...)*" (AR, 2005).

Além disso, o n.º 2 assegura ainda ao titular o direito de "*(...) querendo, tomar conhecimento de todo o processo clínico que lhe diga respeito (...)*". No entanto, a lei prevê exceções em circunstâncias "*(...) devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial, ou de o fazer comunicar a quem seja por si indicado.*", garantindo assim um equilíbrio entre o direito à informação e a salvaguarda da saúde da vítima (AR, 2005).

Desta forma, o artigo reforça o princípio da autodeterminação dos titulares sobre os seus dados de saúde, garantindo que a sua gestão e utilização respeitem a privacidade, a segurança e a finalidade para a qual foram recolhidos.

Após definir a posse e o acesso aos dados, a lei avança para a regulamentação do seu tratamento e proteção, estabelecendo medidas para garantir a segurança, confidencialidade e integridade desta informação. Para tal, o Artigo 4.º detalha as obrigações das entidades responsáveis pelo tratamento dos dados, especificando as condições de acesso, utilização e salvaguarda da informação.

Através do disposto pelo n.º 1, o artigo impõe-se aos responsáveis pelo tratamento a adoção de medidas de proteção da confidencialidade dos dados, garantindo "*(...) a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais*" (AR, 2005).

O n.º 2 vem complementar esta obrigação, determinando que as unidades de saúde devem "*(...) impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança (...)*". Para isso, é necessário cumprir as normas de proteção de dados em vigor, evitando "*(...) destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação*" (AR, 2005).

A segurança da informação é também abordada no n.º 5, ao exigir que os sistemas que armazenam dados de saúde garantam "*(...) a separação entre a informação de saúde e genética e a restante informação pessoal, designadamente através da definição de diversos níveis de acesso*" (AR, 2005).

Por fim, o n.º 6 do mesmo artigo reforça a importância da preservação dos dados, estabelecendo que "*A gestão dos sistemas de informação deve garantir o processamento regular e frequente de cópias de segurança da informação de saúde (...)*", sempre respeitando as regras de confidencialidade previstas na legislação (AR, 2005).

Desta forma, este quarto artigo assegura que o tratamento dos dados de saúde obedece a normas rigorosas de segurança e privacidade, protegendo tanto os titulares como a integridade da informação armazenada pelos diversos sistemas.

Em suma, ainda que a Lei n.º 12/2005, de 26 de janeiro, tenha uma relevância limitada relativamente ao tema em estudo, esta estabelece regras base fundamentais para a proteção e tratamento dos dados de saúde, garantindo segurança, confidencialidade e consentimento na sua utilização. Ao definir direitos para os titulares e responsabilidades para as entidades que tratam esta informação, o documento reforça a necessidade de um controlo rigoroso e estruturado, assegurando um equilíbrio entre a privacidade dos pacientes e a eficácia na prestação de cuidados de saúde.

4.2.3. Deliberação nº 629/2010 da CNPD

As tecnologias de informação e comunicação desempenham um papel essencial na organização e eficiência dos serviços, promovendo a competitividade das empresas e a otimização dos seus processos. No setor das comunicações, estas ferramentas são frequentemente utilizadas para verificar o cumprimento de ordens e instruções, especialmente em relações contratuais, onde a gravação de chamadas pode servir como meio de prova e garantia de execução das transações comerciais (Roque *et al.*, 2007).

No entanto, a gravação de chamadas não se limita ao contexto empresarial. Em situações de emergência, a sua relevância é ainda mais significativa, pois permite o registo de comunicações realizadas para serviços essenciais de socorro. Esta especificidade justificou a sua análise na Deliberação n.º 629/2010 da CNPD, que estabelece princípios e regras para o tratamento destes dados, assegurando que as gravações sejam efetuadas dentro dos limites legais e respeitando os direitos dos cidadãos (Roque *et al.*, 2007).

Embora esta deliberação tenha sido uma referência como instrumento essencial na regulamentação do tratamento de dados pessoais resultantes da gravação de chamadas telefónicas, é importante notar que, atualmente, se encontra desatualizada em algumas afirmações que remetem para a Lei n.º 67/98, de 26 de Outubro (LPD), uma vez que esta veio mais tarde a ser revogada pela Lei n.º 58/2019. No entanto, os princípios e condições estabelecidos mantêm-se em grande parte relevantes, uma vez que as preocupações com a confidencialidade, a finalidade do tratamento e a necessidade de garantir direitos dos titulares continuam a ser eixos centrais da regulamentação vigente.

Assim, este documento abrange três contextos distintos: A) Relação contratual; B) Situação de emergência; C) Monitorização da qualidade do atendimento (Roque *et al.*, 2007). Tendo em conta o âmbito do presente estudo, a análise deste subcapítulo incidirá exclusivamente sobre a segunda categoria.

Relativamente à notificação dos tratamentos, a deliberação começar por destacar que, no contexto das chamadas de emergência, podem ser tratados dados sensíveis, incluindo informações sobre a saúde e, em alguns casos, a vida sexual do titular, enquadrando-se assim no n.º 1 do Artigo 7.º da LPD. Dada a natureza especialmente protegida destes dados, a deliberação esclarece que, "*nos termos da alínea a) do n.º 1 do artigo 28.º da LPD, estes tratamentos carecem de autorização da CNPD*" (Roque *et al.*, 2007). Como consequência, as entidades responsáveis não podem iniciar o tratamento destes dados sem obter essa autorização, que será emitida após a devida notificação e conforme as condições definidas pela referida entidade.

No sentido de estabelecer alguns princípios gerais, o documento aborda o princípio da finalidade como um dos pilares fundamentais da proteção de dados, determinando que "*Os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, pelo que a avaliação sobre a proporcionalidade do tratamento é aferida em função das mesmas*"

(Roque *et al.*, 2007). Além disso, o tratamento deve respeitar os princípios da transparência, reserva da vida privada e conformidade com os direitos e liberdades individuais.

Já o princípio da boa-fé aplica-se tanto aos titulares dos dados como aos trabalhadores que realizam chamadas em nome da empresa. Assim, caso a empresa informe os trabalhadores de que as chamadas serão gravadas, cumprindo as obrigações do Código do Trabalho e do Regime do Contrato de Trabalho em Funções Públicas, considera-se que está a atuar em conformidade com os princípios da transparência e da boa-fé. No entanto, este dever de informação não se confunde com o direito de informação do titular dos dados, previsto pela LPD, que deve ser igualmente garantido (Roque *et al.*, 2007).

Quanto ao responsável pelo tratamento, a deliberação esclarece que, "*Nos casos de situações de emergência, atenta a redação do n.º 4 do artigo 4.º da Lei n.º 41/2004, de 18 de Agosto, o responsável pelo tratamento é o serviço público a quem compete prover auxílio em situações de emergência de qualquer natureza*" (Roque *et al.*, 2007).

De acordo com o Decreto-Lei n.º 167/2003, de 29 de julho, compete ao Instituto Nacional de Emergência Médica coordenar SIEM, o que abrange toda a atividade de urgência e emergência, incluindo o sistema de socorro pré-hospitalar, o transporte, a receção hospitalar e a referenciação do doente/emergente. Adicionalmente, o INEM é também responsável pela formação em emergência médica, pelo planeamento civil e pela gestão da rede de telecomunicações de emergência médica (Roque *et al.*, 2007).

Além disso, o documento esclarece que, no tratamento de dados efetuado por subcontratantes, o contrato ou ato jurídico estabelecido entre o responsável pelo tratamento e a entidade externa deve prever que o subcontratante atua exclusivamente de acordo com as instruções do responsável (Roque *et al.*, 2007). Desta forma, a implementação de medidas técnicas e organizativas adequadas para proteger os dados contra os riscos inerentes ao seu tratamento é uma obrigação da entidade legalmente responsável pela coordenação das emergências.

Não obstante, é importante destacar que as entidades subcontratadas estão vinculadas à obrigação de sigilo profissional, a qual se mantém mesmo após o termo do contrato (Roque *et al.*, 2007).

A finalidade é igualmente um fator determinante na avaliação da admissibilidade e das condições para o tratamento de dados pessoais. Nesse sentido, a deliberação reafirma que,

em situações de emergência, o tratamento desses dados tem como principal objetivo garantir prova do cumprimento das obrigações associadas ao serviço de emergência do respetivo serviço público (Roque *et al.*, 2007).

De seguida, são abordados os direitos dos titulares conferidos pela antiga Lei de Proteção de Dados e, posteriormente, reforçados pelo atual RGPD. No contexto abordado, a deliberação dá destaque à importância do cumprimento do direito à informação. Dado que a prestação de socorro exige uma resposta rápida e eficiente, a obtenção de consentimento individual antes da gravação das chamadas não é viável. Por isso, a diretriz defende que esse direito deve ser assegurado através da inserção de condições gerais de utilização do serviço, cumprindo o dever de transparência por meios acessíveis ao público, como avisos institucionais, sinalização nos serviços de emergência ou outras comunicações informativas (Roque *et al.*, 2007).

Relativamente ao prazo de conservação das chamadas, é esclarecido que, na ausência de um período definido na Lei n.º 41/2004, compete à CNPD estabelecer um limite adequado, tendo em conta a finalidade do tratamento e outras circunstâncias relevantes. Nesse sentido, a Comissão considerou, de forma genérica, que um prazo máximo de 90 dias torna-se suficiente para garantir os objetivos que justificam a recolha e o tratamento das gravações (Roque *et al.*, 2007).

Finalmente, o documento apresenta um conjunto de recomendações de segurança, destacando a necessidade de medidas rigorosas para garantir a proteção dos dados sensíveis envolvidos na gravação de chamadas. Para assegurar a qualidade, integridade e confidencialidade da informação, recomenda-se a implementação de diferentes níveis de acesso, controlados por perfis de utilizador e palavras-passe periodicamente atualizadas. Além disso, deve ser garantido acesso restrito aos servidores do sistema, assegurando que todas as operações sejam registadas para auditoria interna e externa. A realização de cópias de segurança (*backups*) e a sua armazenagem em locais protegidos, acessíveis apenas a técnicos devidamente autorizados, são igualmente medidas essenciais. Independentemente das práticas adotadas, o documento encerra relembrando que a responsabilidade final pela segurança da informação recai sempre sobre a entidade responsável pelo tratamento, que deve assegurar a implementação eficaz destas salvaguardas para prevenir acessos indevidos ou perdas de dados (Roque *et al.*, 2007).

Em suma, embora não se trate de um documento com força legal, esta deliberação assume especial relevância ao estabelecer diretrizes e clarificações sobre aspetos essenciais da legislação vigente antes da entrada em vigor da Lei n.º 58/2019. Ao sistematizar princípios e boas práticas no tratamento de dados em situações de emergência, contribuiu para orientar a aplicação das normas de proteção de dados até à consolidação do atual regime jurídico, que passa agora a ser abordado.

4.2.4. Lei nº 58/2019, de 8 de agosto

Ao contrário das diretivas, que exigem transposição obrigatória para o direito nacional, os regulamentos europeus são diretamente aplicáveis em todos os Estados-Membros, sem necessidade de serem convertidos para as ordens jurídicas nacionais. No entanto, a maioria desses regulamentos pode exigir que cada país introduza ajustes e normas complementares, especialmente em áreas onde há margem de adaptação, como é o caso do regime sancionatório (Ministério Negócios Estrangeiros, 2014).

Assim, de forma a garantir a aplicação eficaz do RGPD em Portugal, tornou-se necessária a criação de um quadro legal que clarificasse as normas e introduzisse adaptações ao contexto nacional. Foi neste sentido que surgiu a Lei n.º 58/2019, de 8 de agosto, com o objetivo de complementar e regulamentar a execução do regulamento, assegurando que as suas disposições fossem aplicadas de forma consistente e alinhada com a realidade jurídica e institucional portuguesa (AR, 2019).

No que diz respeito ao contexto de emergência pré-hospitalar, esta legislação traz várias disposições relevantes, introduzindo normas que influenciam a recolha, armazenamento, partilha e proteção dos dados de saúde. Assim, o presente subcapítulo incidirá sobre as principais diferenças e complementos que esta lei introduz em relação ao RGPD, analisando os artigos mais pertinentes para o estudo.

Relativamente ao âmbito de aplicação, o diploma começa no nº 1 do Artigo 2.º por determinar que abrange todos os "*(...) tratamentos de dados pessoais realizados em território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou subcontratante (...)*". Além disso, a sua aplicação mantém-se válida mesmo quando o tratamento decorre do cumprimento de obrigações legais ou de missões de interesse público. No entanto, a lei também remete para as exclusões já previstas no Artigo

2.º do RGPD, garantindo que não se sobrepõe às limitações e isenções estabelecidas pelo regulamento europeu (AR, 2019).

De seguida, o documento dedica o Capítulo II exclusivamente à Comissão Nacional de Proteção de Dados (CNPD), estabelecendo o seu papel no Artigo 3.º enquanto "*(...) autoridade de controlo responsável pela aplicação do RGPD e da presente lei*". Nesta fase, são definidos os princípios da sua atuação, as suas competências e os deveres de colaboração das entidades públicas e privadas perante esta autoridade de controlo (AR, 2019).

No Artigo 4.º, o diploma reforça ainda a natureza independente da CNPD, determinando que compete à mesma controlar e fiscalizar o cumprimento da legislação nacional e europeia, garantindo "*(...) direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais*" (AR, 2019).

Por fim, o Artigo 8.º estabelece o dever de colaboração das entidades públicas e privadas com a CNPD, determinando que estas devem fornecer todas as informações solicitadas pela autoridade de controlo, incluindo o acesso a sistemas informáticos, ficheiros de dados pessoais e documentação relativa ao tratamento de dados (nº 1 e 2). Este artigo impõe também um dever de sigilo profissional a todos os membros e trabalhadores da CNPD, bem como a quaisquer pessoas mandatadas para exercer funções em seu nome, garantindo que a informação sensível obtida no exercício das suas funções permanece protegida, mesmo após o termo das responsabilidades (nº 3 e 4) (AR, 2019).

Através destas disposições, a lei reforça a importância da CNPD na regulação e supervisão da proteção de dados em Portugal, garantindo que esta autoridade dispõe de mecanismos efetivos para fiscalizar, orientar e sancionar os responsáveis pelo tratamento de dados pessoais.

Já o Capítulo III é dedicado ao Encarregado de Proteção de Dados (EPD), estabelecendo obrigações e funções da sua designação, particularmente em entidades públicas. Assim, o Artigo 10.º reforça que o EPD está "*(...) obrigado a um dever de sigilo profissional em tudo o que diga respeito ao exercício dessas funções, que se mantém após o termo das funções que lhes deram origem*" (nº 1). Além disso, a norma estabelece um dever de confidencialidade para todos os responsáveis pelo tratamento de dados, incluindo subcontratantes e quaisquer pessoas envolvidas no processamento de informações pessoais (nº 2) (AR, 2019).

Quanto às suas funções específicas, o Artigo 11.º atribui ao encarregado responsabilidades adicionais para além daquelas previstas nos Artigos 37.º a 39.º do RGPD. Entre estas, destaca-se: a) a realização de auditorias periódicas ou não programadas; b) a sensibilização dos utilizadores para a importância da deteção de incidentes de segurança; e c) a gestão das interações com os titulares dos dados no âmbito da legislação de proteção de dados (AR, 2019).

No que respeita às entidades públicas, o n.º 1 do Artigo 12.º estabelece a obrigatoriedade da designação de um encarregado, em conformidade com o Artigo 37.º do RGPD. Como exemplo, o diploma inclui os institutos públicos, como o INEM, no conjunto de entidades abrangidas por esta obrigação, assegurando que estas cumprem os requisitos de proteção de dados (AR, 2019).

Estas normas sublinham o papel fundamental do EPD, de forma a assegurar que a sua atuação garante conformidade com as normas nacionais e europeias que reforçam a segurança e a transparência no tratamento de dados pessoais.

A Lei n.º 58/2019 introduziu também algumas disposições inovadoras que complementam o RGPD, adaptando-o a questões específicas do contexto nacional. Entre as alterações mais relevantes, destacam-se as regras relativas ao consentimento de menores e à proteção de dados pessoais de pessoas falecidas.

Já o Artigo 17.º introduz uma proteção inédita dos dados pessoais de pessoas falecidas, garantindo que estes continuam a ser protegidos nos termos do RGPD e da legislação nacional, caso se integrem nas categorias especiais de dados pessoais (como dados de saúde) ou digam respeito à intimidade da vida privada, imagem ou comunicações.

Além disso, nos termos do seu nº 2, o mesmo artigo concede aos herdeiros ou a uma pessoa previamente designada pelo falecido o direito de acesso, retificação e apagamento desses dados. No entanto, permite também que o próprio titular, ainda em vida, determine a impossibilidade de exercício desses direitos após a sua morte, assegurando maior controlo sobre o destino dos seus dados pessoais (nº 3) (AR, 2019).

Mais à frente, o documento introduz regras específicas sobre a conservação de dados pessoais através do Artigo 21.º, estabelecendo critérios para determinar por quanto tempo as informações podem ser armazenadas pelos responsáveis pelo tratamento.

Em primeiro lugar, define-se no nº 1 que o prazo de conservação deve ser aquele fixado por norma legal ou regulamentar. Na ausência de uma regra específica, os dados só podem ser armazenados pelo tempo necessário à prossecução da finalidade para a qual foram recolhidos (AR, 2019).

Além disso, o artigo reforça ainda a obrigação de eliminação dos dados quando deixa de existir a finalidade que justificou o seu tratamento. Desta forma, "*(...) o responsável pelo tratamento deve proceder à destruição ou anonimização*" dos dados, impedindo o seu uso indevido após a cessação da necessidade inicial ou posterior do tratamento (AR, 2019).

Assim, permite-se que os dados não sejam conservados indefinidamente, promovendo um equilíbrio entre a utilidade da informação e a proteção da privacidade dos titulares.

O tratamento de dados de saúde e dados genéticos exige, como se sabe, um nível de proteção reforçado, dado o seu caráter sensível e o impacto que a sua utilização indevida pode ter sobre os titulares. Nesse sentido, o Artigo 29.º estabelece um conjunto de regras e medidas de segurança para garantir a rastreabilidade e proteção dessas informações.

A primeira disposição do artigo determina que o acesso a esses dados deve respeitar o "*(...) princípio da necessidade de conhecer a informação*", ou seja, apenas podem ser consultados por quem realmente precisa deles para desempenhar as suas funções. Além disso, todos os profissionais que lidam com esses dados, incluindo "*(...) trabalhadores e prestadores de serviços do responsável pelo tratamento (...), o encarregado de proteção de dados, os estudantes e investigadores (...)*", estão obrigados a um dever de sigilo, reforçando a proteção contra acessos indevidos ou divulgação não autorizada (n.º 4) (AR, 2019).

Para garantir transparência no acesso aos dados, o diploma estabelece nos termos do nº 6 do mesmo artigo que os titulares devem ser sempre notificados de "*(...) qualquer acesso realizado aos seus dados pessoais (...)*", cabendo ao responsável pelo tratamento assegurar mecanismos de rastreabilidade e notificação que permitam esse controlo (AR, 2019).

Por fim, o artigo prevê através do seu ponto 7 que os requisitos mínimos de segurança para o tratamento de dados de saúde e genéticos sejam definidos por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça. Entre essas medidas incluem-se: a) estabelecimento de permissões de acesso diferenciados; b) requisitos de autenticação prévia de quem acede; e c) registo eletrónico dos acessos e dos dados acedidos (AR, 2019).

A responsabilidade civil das entidades que tratam dados pessoais é reforçada pelo nº 1 do Artigo 33.º, que estabelece que qualquer pessoa afetada por uma violação do RGPD ou da legislação nacional pode exigir compensação ao responsável pelo tratamento ou ao subcontratante pelos prejuízos sofridos (AR, 2019).

No entanto, o artigo também prevê uma exclusão de responsabilidade para os responsáveis pelo tratamento e os subcontratantes, caso estes consigam provar que o dano não lhes é imputável, ou seja, que não tiveram culpa ou que a falha resultou de fatores externos que estes não podiam controlar (n.º 2) (AR, 2019).

Além de estabelecer o direito à reparação por danos decorrentes do tratamento ilícito de dados, a legislação define também um regime sancionatório rigoroso, classificando determinadas contraordenações como muito graves, conforme disposto no Artigo 37.º.

Entre as infrações abrangidas pelo nº 1 incluem-se a violação dolosa dos princípios do tratamento de dados, o tratamento de dados pessoais sem consentimento ou outra base legal válida, o incumprimento das regras sobre dados sensíveis, e a não prestação de informações obrigatórias ao titular dos dados, como as finalidades do tratamento e os destinatários dos dados. Além disso, são igualmente puníveis a recusa em permitir o exercício dos direitos dos titulares, a realização de transferências internacionais de dados em violação do RGPD, e a não colaboração com a CNPD quando solicitada (AR, 2019).

Já as sanções aplicáveis variam de acordo com a dimensão da entidade infratora. No caso de grandes empresas, as coimas podem atingir 20 milhões de euros ou 4% do volume de negócios anual global, aplicando-se limites mais baixos para PME e pessoas singulares (AR, 2019).

Além das contraordenações muito graves, a legislação também prevê um regime sancionatório para infrações classificadas como graves, conforme estabelecido no Artigo 38.º. Estas infrações incluem, entre outras, o incumprimento das obrigações de informação aos titulares de dados, a violação de requisitos de segurança, a falta de registo de tratamentos, o não cumprimento do dever de notificação de incidentes de segurança, e a ausência de avaliações de impacto ou de consulta prévia às autoridades de controlo nos casos exigidos pelo RGPD (AR, 2019).

As sanções aplicáveis variam, novamente, de acordo com a dimensão da entidade infratora, sendo inferiores às previstas para as contraordenações muito graves, mas ainda

assim significativas. No caso de grandes empresas, as coimas podem atingir 10 milhões de euros ou 2% do volume de negócios anual global, com valores mais baixos aplicáveis a PME e pessoas singulares (AR, 2019).

Com estes regimes, a legislação visa garantir a dissuasão de práticas ilícitas, promovendo o cumprimento rigoroso das normas de proteção de dados.

Além das contraordenações já analisadas, a Lei n.º 58/2019 prevê ainda um conjunto de disposições (Artigos 46.º a 54.º) que tipificam diferentes infrações e determinam as respetivas penalizações.

No geral, estes artigos estabelecem que condutas como a utilização ilegítima de dados pessoais, o acesso indevido, o desvio, a destruição, a inserção de registos falsos, a violação de deveres de sigilo e a desobediência perante a CNPD podem configurar crimes puníveis com penas de multa ou prisão, consoante a gravidade da infração. Além disso, a legislação reforça a sua abordagem punitiva ao estabelecer, no Artigo 53.º, que a tentativa é sempre punível nos crimes previstos na presente secção (AR, 2019).

Desta forma, a legislação não apenas regula infrações administrativas e contraordenacionais, mas também prevê responsabilização penal para situações de especial gravidade, garantindo um enquadramento robusto para a proteção dos dados pessoais e dos direitos dos cidadãos.

Quanto às restantes secções, o documento foca-se em matérias de caráter administrativo e legislativo, como disposições finais e transitórias, alterações a outros diplomas legais e normas complementares, que não apresentam um impacto direto para o tema em estudo (AR, 2019).

Em suma, no que respeita aos artigos abordados, verifica-se que Portugal optou por complementar o RGPD com normas próprias, ajustando a sua aplicação a contextos específicos, sem, no entanto, alterar os princípios fundamentais já consagrados pelo regulamento europeu. Assim, a lei reforçou a atuação da CNPD, clarificou o papel do Encarregado de Proteção de Dados, introduziu regras próprias para a conservação e tratamento de dados de saúde, e detalhou um regime sancionatório nacional que distingue contraordenações graves e muito graves, além de prever a responsabilidade penal para crimes relacionados com dados pessoais.

Embora estas disposições tragam maior especificidade e adaptação ao contexto nacional, o essencial do regime de proteção de dados em Portugal continua a seguir integralmente o RGPD, assegurando uma aplicação uniforme das regras dentro do espaço europeu. Desta forma, a Lei n.º 58/2019 assume-se como um instrumento complementar, que não altera a estrutura central do regulamento europeu, mas reforça-o em determinados pontos, garantindo um maior controlo e fiscalização sobre o tratamento de dados pessoais no território nacional.

5. Aplicabilidade ao contexto da emergência pré-hospitalar

Após a análise detalhada do enquadramento normativo europeu e nacional no capítulo anterior, torna-se essencial compreender como estas normas se refletem no contexto da emergência pré-hospitalar. Ao longo do estudo da legislação, verificou-se que, apesar de grande parte das normas analisadas terem sido concebidas tendo em vista o setor da saúde, nem todas possuem uma aplicação tão direta na prática diária das equipas de socorro. Algumas diretivas, como a 2002/58/CE e a 2022/2555, são relevantes para o tema em estudo, mas têm um foco principal nos fornecedores de telecomunicações e na segurança das redes e sistemas, respetivamente. Por outro lado, vários outros documentos contêm disposições que orientam a forma como os profissionais devem atuar no tratamento de dados das vítimas, estabelecendo princípios essenciais para a proteção dessas informações sensíveis.

Além disso, muitas das legislações e regulamentos abordados complementam-se mutuamente, suportando princípios comuns, como a confidencialidade, a segurança e a limitação do tratamento de dados pessoais. Dessa forma, para além de compreender individualmente cada norma, é igualmente importante analisar como estas se interligam e como, em conjunto, estabelecem um quadro jurídico sólido para os profissionais que atuam no contexto da emergência pré-hospitalar.

Deste modo, o presente capítulo centra-se na aplicação prática do regime normativo em vigor, explorando as obrigações legais dos profissionais de emergência, responsáveis pelo tratamento de dados pessoais durante a prestação de socorro, e os direitos e deveres das vítimas, enquanto titulares da informação. A exploração destes aspetos permitirá clarificar como os profissionais devem agir perante diferentes situações de forma a garantir a conformidade com a legislação vigente.

5.1. Obrigações legais dos profissionais

A legislação define um conjunto de princípios e regras fundamentais para o tratamento e proteção de dados pessoais e de saúde, mas a sua aplicação concreta no contexto da emergência pré-hospitalar pode, em alguns casos, suscitar dúvidas devido às especificidades do terreno, onde a diversidade de ocorrências e a necessidade de tomar decisões imediatas influenciam a forma como estas normas são interpretadas e cumpridas.

Nesse sentido, o presente subcapítulo explora algumas das principais obrigações legais dos profissionais de emergência, esclarecendo de que forma os princípios estabelecidos na legislação se refletem na sua atividade. De forma a melhor ilustrar essa aplicação, a Tabela 2 apresenta exemplos práticos de contextos reais, associando cada um ao princípio correspondente e às bases legais que os sustentam.

Tabela 2 – Exemplos práticos de obrigações legais dos responsáveis pelo tratamento

Obrigação	Exemplo Prático Real	Bases Legais
Solicitar o consentimento da vítima	Antes de preencher o verbete com informações pessoais ou de saúde de uma vítima, o profissional deve informá-la e obter o seu consentimento para registar esses dados	Art. 8.º Carta dos Direitos Fundamentais, Art. 6.º RGPD, Art. 16.º Lei n.º 58/2019
Sigilo profissional	Durante e após o serviço, o profissional não pode divulgar dados pessoais ou de saúde que a vítima lhe forneceu sem autorização legal	Art. 9.º e 90.º RGPD, Art. 29.º Lei n.º 58/2019
Informar a autoridade sobre incidentes	Se um equipamento informático que contém o *software iTeams* for roubado, a equipa deve informar a entidade responsável e a CNPD	Art. 33.º RGPD, Art. 23.º Diretiva NIS2
Obter dados de forma lícita	A recolha de dados pessoais fornecidos por familiares, contra a vontade da vítima, viola o princípio da obtenção legal, justa e transparente	Art. 5.º Convenção 108, Art. 5.º RGPD
Limitar as finalidades	A finalidade da recolha de dados pessoais deve limitar-se à prestação de cuidados e o profissional nunca deve utilizar, divulgar ou partilhar esses dados para, por exemplo, fins comerciais	Art. 5.º, 13.º, 14.º e 15.º RGPD, Art. 3 Lei nº 12/2005, Art. 23.º Lei n.º 58/2019
Minimizar os dados	O profissional deve registar dados adequados, pertinentes e limitados ao necessário, descartando informações irrelevantes para o caso específico	Art. 5.º, 25.º e 47.º RGPD
Atualizar os dados	Se a morada atual da vítima mudou recentemente, e não corresponde à registada pela unidade hospitalar, o profissional deve garantir a sua atualização	Art. 5.º RGPD, Art. 4.º Proposta EEDS
Limitar a conservação	Os verbetes devem ser eliminados ou anonimizados após o limite legal estabelecido pelo INEM para a sua conversação	Art. 5.º RGPD, Art. 21.º Lei n.º 58/2019
Garantir a integridade e segurança	Durante a ocorrência, o profissional deve garantir que ninguém, exceto ele mesmo, tem acesso ao verbete ou ao *iTeams*, evitando o acesso ou a alteração de dados	Art. 7.º Convenção 108, Art. 5.º e 32.º RGPD, Art. 29.º Lei n.º 58/2019
Proteção perante inconsciência	Ainda que a vítima se encontre inconsciente, o profissional pode tratar os seus dados sem consentimento explícito	Art. 9.º RGPD

Evitar tratamento de dados especiais	Informações sobre a orientação política, religiosa ou vida sexual da vítima não devem ser recolhidas, a menos que sejam estritamente necessárias para o socorro	Art. 6.º Convenção 108, Art. 9.º RGPD
Utilizar linguagem acessível	O profissional deve comunicar de forma simples e clara informando que os dados serão usados apenas para garantir o melhor atendimento possível e serão protegidos pela lei	Art. 7.º e 12.º RGPD
Fornecer informações sobre a condição da vítima	Sempre que a vítima questionar, o profissional deve informá-la sobre a sua condição de saúde de forma clara e acessível, respeitando o seu direito à informação	Art. 8.º Convenção 108, Art. 8.º Carta Direitos Fundamentais, Art. 3.º Lei nº 12/2005, Art. 15.º RGPD, Art. 3.º Proposta EEDS
Retificar dados, se solicitado	Se a vítima confirmar que a sua morada, ou outro dado pessoal, é diferente da inicialmente fornecida à equipa de socorro, pode solicitar a correção imediata dessa informação ao profissional	Art. 8.º Convenção 108, Art. 8.º Carta Direitos Fundamentais, Art. 5.º, 15.º, 16.º e 19.º RGPD, Art. 17.º Lei n.º 58/2019
Apagar dados, se solicitado	Se a vítima solicitar à equipa que elimine uma determinada informação pessoal, e não houver obrigação legal de a manter, a corporação deve remeter imediatamente o pedido ao responsável pelo tratamento	Art. 8.º Convenção 108, Art. 5.º e 17.º RGPD, Art. 17.º Lei n.º 58/2019
Informar sobre a justificação do tratamento de dados	O profissional deve informar a vítima sobre as finalidades, as categorias, os destinatários e o prazo de conservação relativo ao tratamento realizado aos dados pessoais	Art. 8.º Convenção 108, Art. 3.º Proposta EEDS, Art. 3.º Lei nº 12/2005, Art. 12.º, 13.º e 15.º RGPD, Art. 17.º Lei n.º 58/2019
Avaliar riscos e impactos	Se uma vítima de violência não quiser que o agressor tenha acesso aos seus dados de saúde ou localização, o profissional deve garantir que essa informação não seja partilhada, protegendo a vítima de potenciais represálias	Art. 3.º, 35.º e 36.º RGPD, Art. 7.º Lei n.º 58/2019
Adotar medidas de privacidade e confidencialidade	Ao transmitir um relatório clínico para outra equipa, o profissional deve evitar fazê-lo em locais públicos ou perante pessoas não autorizadas	Art. 5.º, 28.º e 32.º RGPD, Art. 29.º Lei n.º 58/2019
Destruir ou anonimizar os dados para diferentes fins	Se os dados de uma vítima forem utilizados para fins estatísticos, comerciais ou de investigação, a entidade que recolheu os dados deve garantir que todas as informações pessoais sejam anonimizadas antes do tratamento dos dados	Art. 17.º e 89.º RGPD, Art. 21.º e 31.º Lei n.º 58/2019

Zelar pela segurança das comunicações	Na transmissão do estado clínico de uma vítima ou os seus dados pessoais ao CODU, os profissionais devem optar pelo contacto telefónico em vez da comunicação via rádio, garantindo uma maior privacidade na ligação	Art. 5.º Diretiva 2002/58/CE, Art. 32.º RGPD, Art. 17.º Lei n.º 58/2019
Colaborar com a CNPD	Caso a autoridade de controlo realize uma auditoria para avaliar o cumprimento das normas legais, as entidades responsáveis devem colaborar de forma a permitir o acesso aos sistemas e ficheiros, e esclarecendo eventuais dúvidas sobre procedimentos	Art. 31.º RGPD, Art. 8.º Lei n.º 58/2019
Provar que o consentimento foi dado	Sempre que a autoridade de controlo (CNPD) solicite, o responsável pelo tratamento deve conseguir demonstrar que o titular deu o seu consentimento para o tratamento dos dados	Art. 7.º e 28.º RGPD
Informar sobre a possibilidade de remoção do consentimento	Se a vítima deu consentimento para o tratamento dos seus dados, os profissionais devem informá-la de que pode, a qualquer momento, retirar esse consentimento	Art. 7.º e 13.º RGPD, Art. 37.º Lei n.º 58/2019
Informar o titular sobre incidentes	Se uma violação dos dados pessoais for suscetível de implicar um elevado risco para a vítima, o responsável pelo tratamento deve imediatamente comunicar a situação ao titular dos dados	Art. 34.º RGPD

Através da tabela apresentada, procurou-se demonstrar diferentes situações em que os profissionais de emergência devem estar atentos ao cumprimento da legislação aplicável. Além disso, foi dada especial atenção a casos que permitissem enquadrar todos os regulamentos e legislações analisados, de forma a evidenciar a importância de cada um na prática diária das equipas de socorro. Esta diversidade de deveres reflete a complexidade do enquadramento legal aplicado à emergência pré-hospitalar, salientando a necessidade de formação adequada e atualização constante para garantir o cumprimento das regras sem comprometer a eficácia do socorro, nem expor os profissionais a eventuais consequências legais ou disciplinares.

Por fim, importa ainda ressalvar que, perante outras situações que não as enunciadas, os profissionais devem sempre garantir um equilíbrio entre a proteção da privacidade da vítima e a salvaguarda da sua condição de vida, assegurando que qualquer tratamento de dados pessoais respeita os princípios fundamentais de privacidade e segurança.

5.2. Direitos das vítimas

Para além de conhecerem as suas obrigações legais, os responsáveis pelo tratamento de dados no contexto da emergência pré-hospitalar podem beneficiar de uma compreensão mais ampla ao também analisarem os direitos das vítimas. Estes direitos não só justificam muitas das obrigações impostas aos profissionais, como também voltam a reforçar a necessidade de garantir que qualquer tratamento de informação pessoal ou sensível seja realizado de forma transparente e segura.

Nesse sentido, adotando uma abordagem alinhada com a do subcapítulo anterior, este segmento apresenta, através da Tabela 3, exemplos reais que ilustram como os direitos das vítimas são exercidos na prática, associando-os às bases legais que os sustentam.

Tabela 3 – Exemplos práticos de direitos e deveres dos titulares dos dados

Direitos	Exemplo Prático Real	Bases Legais
Respeito pela vida privada e familiar	Durante uma ocorrência em ambiente domiciliário, a equipa de socorro deve evitar expor informações clínicas diante de vizinhos ou terceiros, garantindo a privacidade da vítima e da sua família	Art. 12.º DUDH, Art. 8.º CEDH, Art. 7.º CDF da UE
Conhecer a justificação do tratamento	Antes do profissional recolher os dados, a vítima tem o direito de ser informada sobre as finalidades, as categorias, os destinatários e o prazo de conservação relativo ao tratamento realizado a essas informações sensíveis	Art. 8.º Convenção 108, Art. 3.º Proposta EEDS, Art. 3.º Lei nº 12/2005, Art. 12.º, 13.º e 15.º RGPD, Art. 17.º Lei n.º 58/2019
Dar o seu consentimento	Antes do registo e tratamento dos dados de saúde no verbete ou no *iTeams*, a vítima tem o direito de consentir ou não relativamente à realização dessas operações	Art. 8.º Carta dos Direitos Fundamentais, Art. 6.º RGPD, Art. 16.º Lei n.º 58/2019
Retirar o seu consentimento	Uma vítima que tenha inicialmente consentido no registo dos seus dados para efeitos de cuidados de saúde pode, posteriormente, solicitar a remoção dos mesmos, caso a finalidade seja alterada para fins estatísticos, comerciais, de investigação, entre outros	Art. 7.º e 13.º RGPD, Art. 37.º Lei n.º 58/2019
Ter os seus dados protegidos	Após a ocorrência, as informações pessoais e de saúde da vítima devem ser guardadas em locais seguros e acessíveis apenas a profissionais autorizados	Art. 7.º Convenção 108, Art. 5.º e 32.º RGPD, Art. 29.º Lei n.º 58/2019

Realizar chamadas de socorro com confidencialidade	Se uma vítima ligar para o 112 a solicitar ajuda, os seus dados pessoais e a gravação da chamada devem ser mantidos em sigilo e apenas utilizados para fins de gestão da emergência	Art. 5.º Diretiva 2002/58/CE, Art. 14.º Lei n.º 41/2004, Art. 32.º RGPD, Art. 17.º Lei n.º 58/2019
Acesso, oposição, retificação, apagamento, limitação, portabilidade	Durante e após a emergência, a vítima pode solicitar o acesso, a retificação e/ou o apagamento dos dados. Além disso, pode ainda pedir a limitação das finalidades e a portabilidade dos dados, ou ainda opor-se ao tratamento dos mesmos	Art. 8.º CDF da UE, Art. 3.º Proposta EEDS, Art. 15.º, 16.º, 17.º, 18.º, 20.º e 21.º RGPD
Reclamar à autoridade de controlo	Se a vítima considerar que os seus dados foram indevidamente utilizados ou partilhados sem autorização, pode apresentar uma reclamação à CNPD	Art. 12.º, 13.º, 14.º e 15.º RGPD
Ter os seus dados protegidos perante inconsciência	Ainda que a vítima se encontre inconsciente ou incapaz de consentir, a legislação permite que os dados sejam tratados sem consentimento explícito	Art. 9.º RGPD
Tomar conhecimento do processo clínico	Sempre que desejar, a vítima tem o direito de ser informada sobre a sua condição de saúde de forma clara e acessível, respeitando o seu direito à informação	Art. 8.º Convenção 108, Art. 8.º Carta Direitos Fundamentais, Art. 3.º Lei nº 12/2005, Art. 15.º RGPD, Art. 3.º Proposta EEDS
Pedir a uma entidade que apresente reclamação por si	Caso pretenda, o titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, para, em seu nome, apresentar reclamação à autoridade de controlo	Art. 57.º e 80.º RGPD, Art. 37.º Lei n.º 58/2019
Ter os seus dados protegidos após falecimento	Mesmo após falecimento, a intimidade da vida privada, imagem, dados relativos às comunicações e categorias especiais de dados pessoais da vítima devem continuar a ser protegidos, nos termos da lei	Art. 17.º Lei n.º 58/2019
Conceder direitos a herdeiros	Antes do seu falecimento, qualquer vítima pode indicar uma pessoa ou, na sua falta, um herdeiro que tenha direito a aceder às suas informações médicas para resolver, por exemplo, questões legais ou de saúde familiar	Art. 17.º Lei n.º 58/2019
Ser notificado sobre incidentes	Qualquer incidente que ocorra envolvendo os dados pessoais da vítima e que a coloque num elevado risco de perigo, deve ser comunicado à mesma sem demora injustificada	Art. 34.º RGPD

Ter os seus dados atualizados	Caso um documento ou sistema informático contenha informações desatualizadas que possam comprometer o tratamento da vítima, esta pode solicitar uma atualização	Art. 5.º RGPD, Art. 4.º Proposta EEDS
Ser compensado pelo responsável dos prejuízos	Se um serviço de emergência divulgar indevidamente os dados de uma vítima e isso lhe causar danos, esta pode exigir uma compensação pelos prejuízos sofridos	Art. 33.º RGPD
Não ser sujeito a decisões automatizadas	A avaliação da necessidade de transporte hospitalar não pode ser feita apenas por sistemas automatizados, sendo sempre necessária a intervenção humana	Art. 22.º RGPD
Conhecer quem acedeu aos dados	A vítima pode solicitar uma listagem dos profissionais que acederam ao seu processo clínico no sistema de registos de saúde eletrónico	Art. 3.º Proposta EEDS, Art. 29.º Lei n.º 58/2019

Através da tabela anterior, procurou-se demonstrar diferentes situações em que os direitos das vítimas de emergência pré-hospitalar devem ser salvaguardados, ilustrando como a legislação aplicável se traduz em garantias concretas de proteção da sua privacidade e dignidade. Tal como feito no subcapítulo anterior, foi dada especial atenção a exemplos que permitissem enquadrar todos os regulamentos e legislações analisados, de forma a reforçar a importância de cada um no contexto das operações de socorro.

A diversidade de normas revela, uma vez mais, a complexidade do enquadramento legal que rege o tratamento de dados na saúde, destacando a necessidade de as equipas de emergência não só conhecerem as suas obrigações, mas também compreenderem e respeitarem os direitos das vítimas.

Importa ainda sublinhar que, paralelamente a estes direitos, as vítimas de situações de emergência têm também deveres fundamentais que contribuem para o bom funcionamento do sistema de socorro. Entre eles destacam-se a responsabilidade de fornecer informações precisas e completas aos profissionais de saúde, respeitar os direitos e as instruções das equipas de emergência e, nos casos de recusa de cuidados ou transporte, formalizar essa decisão através de documento próprio com a devida identificação pessoal.

Por fim, deve novamente ser recordado que, mesmo perante situações não enunciadas nesta tabela, a atuação das equipas deve sempre assegurar um equilíbrio entre a proteção da privacidade das vítimas e a salvaguarda da sua condição de vida, respeitando os princípios fundamentais de privacidade, segurança e dignidade que norteiam o tratamento de dados pessoais em contexto de saúde.

6. Caso de estudo

Além da análise teórica do enquadramento normativo e da sua aplicação prática no contexto da emergência pré-hospitalar, este projeto definiu, desde o início, como principais objetivos a avaliação dos procedimentos e do nível de consciencialização dos profissionais de emergência quanto ao tratamento e proteção de dados.

Nesse sentido, a última fase deste trabalho compreende a realização de um caso de estudo que permita validar a aplicação dos princípios e obrigações. Entende-se por caso de estudo uma abordagem de investigação centrada na análise aprofundada de uma situação específica, em contexto real e concreto, com foco em compreender fenómenos complexos, identificar práticas, desafios e oportunidades de melhoria, bem como fornecer uma visão detalhada sobre a realidade observada (Hollweck, 2015).

A utilização de estudos de caso revela-se particularmente relevante em áreas onde as práticas operacionais, como é o caso da emergência pré-hospitalar, exigem uma adaptação constante das normas jurídicas às condições reais de atuação. Neste contexto, a análise de comportamentos face a situações específicas permite complementar a abordagem normativa e teórica realizada anteriormente, oferecendo uma perspetiva prática sobre o conhecimento e a aplicação das obrigações legais de proteção de dados por parte dos profissionais de socorro. Além disso, possibilita também identificar os principais desafios e limitações enfrentados no cumprimento dessas obrigações, bem como recolher sugestões de melhoria com base na experiência prática dos intervenientes.

Assim, o presente capítulo, dividido em metodologia, resultados e análise comparativa, começa por explorar as características do questionário desenvolvido, passando depois para a análise da amostra e dos resultados estatísticos obtidos.

6.1. Metodologia

De forma a garantir a validade e fiabilidade dos resultados obtidos, torna-se essencial estabelecer uma metodologia rigorosa que oriente todas as etapas da investigação. Nesse sentido, e com base numa abordagem semelhante à adotada na revisão de literatura, uma análise exploratória preliminar foi realizada com o objetivo de identificar a existência de questionários ou outros instrumentos de inquérito que pudessem ser adaptados ao contexto específico da emergência pré-hospitalar. Para esse efeito, realizaram-se pesquisas

sistemáticas em diversas bases de dados e plataformas de investigação académica, tais como *Google Scholar*, *Scopus*, *b-on*, JSTOR, EBSCO e *ResearchGate*, recorrendo a termos-chave relacionados com a proteção de dados em cenários de emergência médica.

Não obstante a diversidade de fontes consultadas, não foi possível identificar instrumentos de avaliação que abordassem, de forma direta, a aplicação das normas de proteção de dados pessoais neste domínio. Tal inexistência reforçou a necessidade de desenvolver um questionário original e devidamente ajustado à realidade operacional das equipas de emergência pré-hospitalar.

A definição clara da estratégia metodológica permite não apenas assegurar a coerência e a objetividade do estudo, mas também garantir que os procedimentos adotados sejam replicáveis e ajustados ao contexto em análise. Neste caso, a estratégia adotada seguiu um conjunto estruturado de fases:

1. **Identificação dos objetivos** a alcançar com o estudo, estabelecendo os aspetos específicos a serem avaliados;
2. **Estruturação do questionário**, garantindo a adequação das perguntas ao tema em estudo e a recolha eficaz de respostas relevantes;
3. **Divulgação do questionário** junto da amostra-alvo, utilizando canais apropriados para alcançar diferentes profissionais da emergência pré-hospitalar;
4. **Recolha dos resultados** de forma anónima e organizada, respeitando as normas éticas e de proteção de dados;
5. **Análise dos resultados** de forma a identificar tendências, padrões e discrepâncias nos dados recolhidos;
6. **Discussão e retirada de conclusões**, avaliando os resultados à luz da revisão de literatura, do enquadramento normativo e das práticas no terreno.

Tendo em conta o objetivo central proposto para esta etapa do estudo, foi adotado o método quantitativo para a análise dos dados, uma abordagem amplamente reconhecida pela sua capacidade de medir e quantificar fenómenos sociais de forma objetiva e sistemática. Esta metodologia foi escolhida por permitir a recolha e análise de dados numéricos, oferecendo uma visão clara da frequência e distribuição de determinadas atitudes, comportamentos ou opiniões entre os profissionais de emergência. Além disso, o método quantitativo facilita a generalização dos resultados a partir de uma amostra representativa, assegurando maior rigor e validade estatística (Grand Canyon University, 2023).

6.1.1. Instrumento de recolha de dados

No âmbito desta metodologia, tornou-se fundamental selecionar o instrumento de recolha de dados mais adequado para assegurar uma abordagem estruturada e sistemática na obtenção de informações relevantes para o estudo. Optou-se, assim, pela aplicação de questionários eletrónicos, dada a sua capacidade de alcançar um número significativo de participantes de forma prática e eficiente. Este método facilita ainda a preservação do anonimato e da confidencialidade das respostas, fatores essenciais para garantir a fiabilidade e a honestidade dos dados recolhidos. A realização de inquéritos por meio de questionários digitais revelou-se, portanto, a solução mais indicada para avaliar o nível de conhecimento, perceções e práticas dos profissionais face à proteção de dados no contexto em análise.

Como ferramenta de desenvolvimento e gestão dos questionários, foi utilizado o *Microsoft Forms*, que se destaca pela simplicidade na criação, distribuição e recolha de respostas. Adicionalmente, esta solução assegura a conformidade com as normas de proteção de dados, uma vez que impede a recolha de dados pessoais não autorizados, garantindo o anonimato dos participantes e a confidencialidade das respostas.

A escolha do *Microsoft Forms* deveu-se também à sua facilidade de acesso e utilização, permitindo que os profissionais de emergência, independentemente da sua localização geográfica ou nível de literacia digital, pudessem participar de forma simples e rápida.

Por fim, a plataforma disponibiliza ainda funcionalidades de análise preliminar dos dados, que facilitam a organização e interpretação dos resultados para a fase subsequente do estudo.

6.1.2. Estrutura do questionário

Recorrendo ao *Microsoft Forms*, foi criado um questionário em branco, no qual se iniciou a construção de uma mensagem dirigida aos participantes, com o objetivo de apresentar de forma clara e transparente todas as informações relevantes para a participação no estudo. Esse texto inclui a identificação do autor e do professor orientador, o enquadramento académico do questionário no âmbito da dissertação de mestrado, bem como a explicitação dos objetivos do estudo. Além disso, é reforçada a garantia de que a participação é anónima, livre e voluntária, assegurando aos participantes a possibilidade de, a qualquer momento, desistirem ou revogarem a autorização para a utilização das suas respostas. Por fim, é também indicado o tempo médio necessário para a conclusão do

questionário e disponibilizado o contacto de email do autor para o esclarecimento de eventuais dúvidas.

Após a introdução, o questionário (Apêndice A – Questionário sobre Tratamento e proteção de dados na emergência pré-hospitalar) foi organizado em cinco secções principais, dispostos de forma lógica e sequencial, de modo a facilitar a compreensão por parte dos participantes e garantir a recolha estruturada de dados relevantes. Cada secção aborda um aspeto específico do tema em análise:

1. **Consentimento informado, livre e esclarecido:** O participante manifesta a sua concordância em participar no estudo ao declarar que leu e compreendeu a informação apresentada na introdução, aceitando fazê-lo de forma voluntária, livre e esclarecida. Com este procedimento, garante-se o cumprimento das normas éticas e das disposições legais em matéria de proteção de dados;
2. **Caracterização sociodemográfica:** Informações básicas sobre o perfil dos participantes são recolhidas, incluindo género, faixa etária, escolaridade, região, tempo de serviço e vínculo institucional. Estes dados permitem contextualizar os resultados e analisar eventuais variações com base no perfil sociodemográfico da amostra;
3. **Perceção sobre a legislação vigente:** A perceção geral dos profissionais relativamente ao conhecimento da legislação vigente em matéria de proteção de dados é avaliada através de questões que abordam o seu grau de familiaridade com conceitos base de normas aplicáveis, bem como se já frequentaram alguma formação nesta área e há quanto tempo a realizaram;
4. **Avaliação de conhecimentos práticos:** É realizada uma análise dos conhecimentos práticos dos profissionais sobre as obrigações legais e operacionais que regem o tratamento de dados pessoais durante a prestação de cuidados de emergência. Inclui questões sobre procedimentos de consentimento, segurança na transmissão de dados, acesso à informação e cumprimento das normas de confidencialidade;
5. **Desafios e melhorias:** Solicita-se aos participantes que identifiquem as principais dificuldades sentidas no terreno no que respeita à aplicação das normas legais. Adicionalmente, pretende-se que indiquem as principais sugestões ou propostas de melhoria que consideram relevantes para reforçar a proteção de dados no setor da emergência pré-hospitalar.

Ao nível da composição interna, todas as secções possuem maioritariamente questões de formato estruturado e fechado, predominantemente de escolha múltipla, onde uma ou mais respostas estão certas e as restantes estão erradas. O conjunto de opções de resposta foi criteriosamente definido de forma a permitir avaliar, com um elevado grau de fiabilidade, duas dimensões fundamentais para a análise: por um lado, a profundidade do conhecimento demonstrado pelos inquiridos em relação a cada tema, medida pelo número e conteúdo das respostas corretas selecionadas; por outro lado, o grau de clareza e compreensão dos conceitos específicos associados à legislação, aferido através da identificação das respostas incorretas assinaladas.

Na última secção, dedicada à identificação de desafios e sugestões de melhoria, foram incluídas, para além das questões de resposta fechada, duas perguntas em formato de resposta em texto livre, que permitem aos participantes indicar exemplos ou propostas adicionais que não se encontrem previstos nas opções previamente apresentadas. Esta abordagem permite recolher contributos mais personalizados e relevantes, considerando que a identificação de desafios e propostas de melhoria constitui um dos principais objetivos finais deste projeto. Ao incluir perguntas de resposta em texto livre, cria-se a oportunidade para que os profissionais partilhem a sua experiência direta e opiniões próprias, superando as limitações das respostas pré-definidas, que podem não contemplar todas as realidades ou perspetivas vividas no terreno.

De modo a facilitar a compreensão de todos os inquiridos, procurou-se adotar uma linguagem clara, simples e acessível em todas as perguntas e instruções do questionário, evitando a utilização de termos excessivamente técnicos ou jurídicos que pudessem dificultar a participação ou gerar interpretações ambíguas.

Além disso, o tempo estimado para a sua conclusão foi cuidadosamente considerado, procurando-se que a duração não excedesse os 10 minutos, de forma a não desmotivar a participação dos profissionais. Para complementar esta medida, foi ainda ativada a barra de progresso no questionário, permitindo aos participantes acompanhar facilmente o seu avanço e gerirem melhor o tempo até à conclusão.

6.1.3. População e amostra expectável

A definição da população-alvo e da amostra é uma etapa fundamental para garantir a representatividade e a validade dos dados recolhidos no estudo. Considerando os objetivos

do presente projeto, o questionário foi dirigido especificamente a profissionais que atuam no contexto da emergência pré-hospitalar, dado o papel central que estes desempenham no tratamento de dados pessoais e de saúde em situações de socorro.

A população-alvo é, assim, composta por profissionais de emergência médica em Portugal, abrangendo diferentes entidades e serviços que integram o Sistema Integrado de Emergência Médica. Pretende-se incluir participantes de diversas categorias profissionais, de modo a obter uma visão abrangente das práticas e perceções sobre a proteção de dados pessoais no setor. Pretende-se, por isso, que respondam ao questionário profissionais do INEM, das corporações de Bombeiros e de delegações da CVP, sejam eles TAS, TAT ou TEPH, elementos das equipas médicas de emergência e reanimação, operadores do CODU, e demais carreiras profissionais que desempenhem funções no atendimento e no transporte de vítimas em situação de urgência ou emergência. Esta diversidade permitirá captar diferentes níveis de experiência, formação e perceções sobre a proteção de dados, promovendo uma análise mais completa e representativa das realidades vividas no terreno.

Não obstante a preocupação com a diversidade da população-alvo, reconhece-se que a utilização de um método de amostragem por conveniência, baseado na acessibilidade e na adesão voluntária e aleatória dos participantes, poderá limitar a representatividade estatística dos resultados. Ainda assim, a informação recolhida constitui um contributo valioso para compreender o estado atual da consciencialização e das práticas de proteção de dados no contexto da emergência pré-hospitalar.

Relativamente à amostra expectável, prevê-se recolher entre 50 a 100 respostas, número considerado adequado para obter uma primeira visão exploratória sobre o tema em análise. Esta amostra permite identificar padrões de conhecimento, perceções e práticas dos profissionais relativamente à proteção e tratamento de dados pessoais nas operações de emergência pré-hospitalar, assim como recolher contributos relevantes para a identificação de desafios e sugestões de melhoria neste domínio.

6.1.4. Pré-teste do questionário

Antes de ser divulgado, qualquer inquérito deve ser sujeito a um rigoroso processo de pré-teste prévio, que permita assegurar que o mesmo se encontra devidamente ajustado ao objetivo do estudo e ao perfil do público-alvo, promovendo assim a qualidade, a fiabilidade e a credibilidade dos dados a recolher.

Para esse efeito, o instrumento desenvolvido foi submetido a um processo de pré-teste prático, que consistiu na aplicação do questionário a quatro profissionais da área da emergência pré-hospitalar, selecionados com base em perfis distintos. Embora partilhassem algumas características em comum - nomeadamente a região de atuação (Centro) e o nível de escolaridade (ensino superior) - os revisores diferiam quanto ao vínculo institucional (profissional/voluntário), formação, faixa etária e tempo de serviço. Esta diversidade permitiu obter *feedback* representativo de diferentes realidades do terreno.

No mesmo dia, cada um dos profissionais completou integralmente o questionário como se de um inquirido real se tratasse. Após a sua submissão, foi-lhes solicitado o preenchimento da Tabela 4, concebida para recolher as suas opiniões de forma estruturada com base em critérios como clareza, relevância, linguagem, coerência, duração e nível de dificuldade das questões.

Tabela 4 – *Feedback* dos revisores no processo de validação do questionário

	Revisor 1	**Revisor 2**	**Revisor 3**	**Revisor 4**
Profissão/Formação, entidade e vínculo	Enfermeiro/a INEM (Profissional)	Enfermeiro/a Bombeiros (Voluntário)	TAS Bombeiros (Profissional)	TAT Bombeiros (Voluntário)
Tempo de realização (em min.)	9.20	6.10	10.30	8.30
Explicação de objetivos e direitos	Claro	Claro	Claro	Claro
Pertinência das perguntas	Pertinentes	Pertinentes	Pertinentes	Pertinentes
Clareza das perguntas	Claras	Claras	Média	Média
Dificuldade das perguntas	Média	Média	Média	Média
Ordem e fluxo das secções e perguntas	Coerente	Coerente	Coerente	Coerente
***Design* e usabilidade da plataforma**	Boa	Boa	Boa	Boa
Perceção de anonimato	Não identificável	Não identificável	Não identificável	Não identificável
***Feedback* geral e melhorias sugeridas**	Nada a anotar	Simplificar a construção frásica	Nada a anotar	Vocabulário mais acessível

A análise dos dados obtidos através da Tabela 4 permitiu melhorar diversos aspetos essenciais à qualidade do questionário. Relativamente ao tempo médio de realização, este foi de 8,5 minutos, o que confirma a estimativa inicial de que o inquérito poderia ser completado em cerca de 10 minutos, sem comprometer a motivação dos participantes.

No que respeita à explicação dos objetivos do estudo e dos direitos dos participantes, bem como à pertinência e clareza das perguntas, todos os revisores concordaram que os conteúdos apresentados eram adequados, compreensíveis e diretamente relacionados com o tema em estudo.

Quanto ao grau de dificuldade das questões, todos os profissionais classificaram-no como médio, resultado especialmente relevante tendo em conta a necessidade de garantir que o questionário permanece acessível a diferentes níveis de conhecimento e experiência profissional. Por outro lado, a ordem das secções e a sequência das perguntas foram igualmente bem avaliadas, tendo sido consideradas coerentes e de leitura fluída.

A usabilidade da plataforma *Microsoft Forms* também mereceu avaliação positiva por parte dos quatro revisores. Importa ainda destacar que todos os participantes confirmaram que, em nenhum momento, o questionário permite a sua identificação individual com base nas perguntas colocadas, o que reforça o cumprimento dos princípios de anonimato e proteção da privacidade.

Por fim, o *feedback* geral foi positivo, tendo apenas dois dos revisores sugerido pequenas melhorias ao nível da construção frásica de algumas questões, de forma a torná-las mais simples e acessíveis a todos os participantes. Tendo em conta essas opiniões, procedeu-se à reformulação pontual de determinadas frases, com o objetivo de tornar a linguagem mais clara, direta e compreensível, sem comprometer o rigor ou a intenção original das perguntas. Nenhuma outra alteração foi realizada ao questionário.

Para além da análise qualitativa das opiniões dos revisores, é igualmente pertinente observar as suas respostas ao questionário (Apêndice C – Transcrição integral das respostas recolhidas dos revisores), uma vez que tal permite antecipar tendências e aferir, de forma preliminar, qual o grau de consciencialização, bem como os principais desafios e propostas de melhoria que uma eventual amostra alargada de profissionais poderá vir a identificar.

Nesse sentido, começa-se por apresentar uma lista das principais estatísticas obtidas na secção dedicada à perceção sobre a legislação vigente:

- **25%** dos participantes afirmaram não conhecer a regulamentação europeia e nacional sobre proteção de dados. **75%** indicaram ter apenas conhecimento parcial;
- **50%** afirmaram já ter frequentado formação específica sobre proteção de dados, enquanto os restantes **50%** nunca tiveram qualquer formação;
- **100%** dos revisores que tiveram formação (2) referiram que esta foi promovida pela própria instituição de trabalho;
- **25%** indicaram não saber distinguir um conjunto de dados pessoais de dados sensíveis, enquanto os restantes **75%** revelaram não ter certeza;
- **25%** afirmaram, de forma incorreta, que o consentimento é sempre necessário. Os restantes **75%** demonstraram maior conhecimento ao referirem que nem sempre é exigido;
- **50%** tinham ouvido falar do princípio da minimização dos dados, mas sem certezas quanto ao seu conteúdo; os restantes **50%** nunca ouviram falar do mesmo.

Relativamente à secção dedicada à avaliação de conhecimentos práticos através de cenários reais, os resultados obtidos pelos revisores permitem aferir, de forma indicativa, quais os princípios que aparentam estar mais consolidados e quais aqueles que revelam maiores lacunas de compreensão ou aplicação. A análise dos dados permitiu destacar os seguintes pontos:

- **75%** dos revisores afirmam que, perante uma vítima consciente, devem obter o consentimento antes de recolher dados, exceto se estiver em causa uma obrigação legal ou interesse vital;
- Apenas **25%** identificaram corretamente a conduta a adotar no momento de partilha de informações com familiares, demonstrando fragilidades no entendimento dos limites da confidencialidade em contexto de emergência;
- **50%** escolheram corretamente o meio de comunicação mais seguro para transmitir dados ao CODU, refletindo conhecimento moderado sobre segurança nas comunicações;
- Também **50%** acertaram na abordagem correta sobre o armazenamento de apontamentos com dados pessoais após a ocorrência, evidenciando dúvidas quanto às práticas de conservação de dados;

- A totalidade dos revisores (**100%**) reconheceu corretamente os elementos de informação obrigatórios a prestar ao titular antes da recolha dos dados, revelando um entendimento sólido sobre o dever de transparência;
- Nenhum dos revisores (**0%**) indicou corretamente o procedimento adequado para comprovar que o consentimento foi dado, o que aponta para uma lacuna importante na compreensão sobre a rastreabilidade e prova legal do consentimento;
- **100%** responderam corretamente sobre o direito de remoção do consentimento, revelando sensibilidade quanto à autonomia do titular dos dados;
- **75%** souberam identificar corretamente a atitude a adotar face a um pedido de informação por parte de um jornalista, o que demonstra atenção aos limites do dever de sigilo profissional;
- **75%** responderam corretamente quanto à partilha de dados com agentes da autoridade, reconhecendo o enquadramento legal e o dever de colaboração nestes casos.

De forma global, cerca de 61% das respostas dadas na secção dos cenários práticos foram corretamente selecionadas pelos revisores, sugerindo que, embora exista algum domínio prático de certos princípios, persistem fragilidades em áreas críticas como a partilha de dados com terceiros, a conservação da informação e a demonstração formal do consentimento.

Estes dados preliminares, se projetados para uma amostra de, por exemplo, 200 profissionais, indicariam que cerca de 78 destes não responderiam corretamente à maioria dos cenários práticos propostos, evidenciando uma necessidade urgente de reforçar a formação prática e de clarificar procedimentos operacionais no terreno, sobretudo no que diz respeito à aplicação concreta dos princípios legais de proteção de dados.

6.1.5. Estratégia de divulgação

Após a definição dos objetivos do estudo, da metodologia aplicada e da estrutura do questionário, tornou-se essencial garantir que a recolha de dados seja realizada de forma eficaz, através de uma estratégia de divulgação bem planeada. Esta etapa reveste-se de particular importância, uma vez que a qualidade dos resultados depende diretamente da capacidade de alcançar um número representativo de profissionais de emergência pré-hospitalar, assegurando a diversidade e a fiabilidade da amostra.

Neste sentido, a abordagem adotada para a divulgação do questionário visou maximizar o seu alcance junto da comunidade da emergência e socorro, recorrendo a diferentes canais de comunicação que promovem a participação e garantem a representatividade da amostra:

- **Correio eletrónico** (Apêndice B – Email de divulgação do questionário), dirigido a contactos institucionais com capacidade de promover a partilha interna junto dos seus colaboradores, nomeadamente o INEM, as corporações de Bombeiros e as delegações da CVP;
- **Redes sociais**, através de publicações e partilhas em grupos específicos de profissionais nas plataformas *Facebook*, *Telegram* e *WhatsApp*, permitindo alcançar aqueles que, por vezes, não consultam regularmente o correio eletrónico institucional, mas que mantêm uma presença ativa nestes canais informais;
- **Comunicação direta** com profissionais da área, recorrendo à rede de contactos pessoais estabelecida no exercício das funções de Bombeiro voluntário, promovendo uma divulgação mais próxima e personalizada, especialmente junto dos colegas da própria corporação.

Com a combinação destes três métodos de divulgação, procurou-se garantir um alcance abrangente e eficaz junto dos profissionais da emergência pré-hospitalar, maximizando a participação no estudo. Para reforçar esse objetivo, o inquérito esteve disponível durante três semanas, com um período de recolha compreendido entre os dias 1 e 20 de abril, com a possibilidade de prolongamento caso a amostra desejada não fosse atingida. Durante esse intervalo, foram ainda realizados reenvios e lembretes periódicos, nomeadamente com frequência semanal, incentivando a participação contínua e reforçando o envolvimento de potenciais inquiridos que ainda não tivessem respondido.

6.2. Resultados

O questionário aplicado esteve disponível durante o período previamente estipulado, tendo-se, nesse intervalo, registado um total de 143 respostas válidas. Este número ultrapassou significativamente as expectativas inicialmente definidas, que apontavam para a recolha de entre 50 e 100 respostas, o que se deve, em grande parte, à partilha exaustiva realizada nos diferentes meios de comunicação identificados no subcapítulo 6.1.5, promovida de forma contínua ao longo de todo o período em que o inquérito esteve ativo.

Quanto ao tempo médio de preenchimento do questionário, os inquiridos levaram, em média, 13.17 minutos a completar a totalidade das questões, um valor ligeiramente superior ao estimado aquando da elaboração do inquérito. Tal poderá indicar que a maioria dos participantes dedicou atenção e reflexão às respostas, contribuindo para uma recolha de dados mais rica e cuidada.

Para a análise dos resultados, foram utilizados dois instrumentos principais: por um lado, o painel de análise automática disponibilizado pela própria plataforma *Microsoft Forms*, o qual apresenta de forma visual e estatística os dados recolhidos, através de gráficos de barras, gráficos circulares e indicadores percentuais; por outro lado, procedeu-se também à exportação de um ficheiro Excel (Apêndice D – Transcrição integral das respostas recolhidas de todos os participantes) contendo todas as respostas individuais, permitindo uma análise mais detalhada e personalizada das tendências e distribuições observadas.

A partir destes dois recursos, e tendo sempre por base uma abordagem descritiva e global, foram realizadas nesta fase análises estatísticas elementares - tais como frequências absolutas, percentagens, médias e distribuições - com o propósito de compreender as perceções gerais dos inquiridos. Como tal, os resultados a seguir apresentados não devem ser vistos como conclusivos ou universais, mas como indicadores valiosos de tendências e realidades práticas, capazes de sustentar reflexões e debates futuros sobre a proteção de dados neste contexto específico.

Importa reforçar que, em nenhum momento, foi feita qualquer análise individualizada das respostas, garantindo-se a confidencialidade e anonimato dos participantes, conforme previsto nos princípios éticos delineados para o estudo.

Por fim, a estrutura deste subcapítulo segue de forma direta a organização do próprio questionário, estando as divisões seguintes alinhadas com as diferentes secções temáticas que o compõem. Esta estrutura permite uma leitura mais fluida e coerente dos dados, favorecendo uma compreensão sistemática das conclusões a retirar.

6.2.1. Caracterização da amostra

A primeira secção do questionário diz respeito à caracterização sociodemográfica dos participantes. Nesse sentido, a Figura 10 ilustra o género da totalidade dos inquiridos, onde é possível verificar que 91 (64%) participantes são do sexo masculino, enquanto 51 (36%) são do sexo oposto.

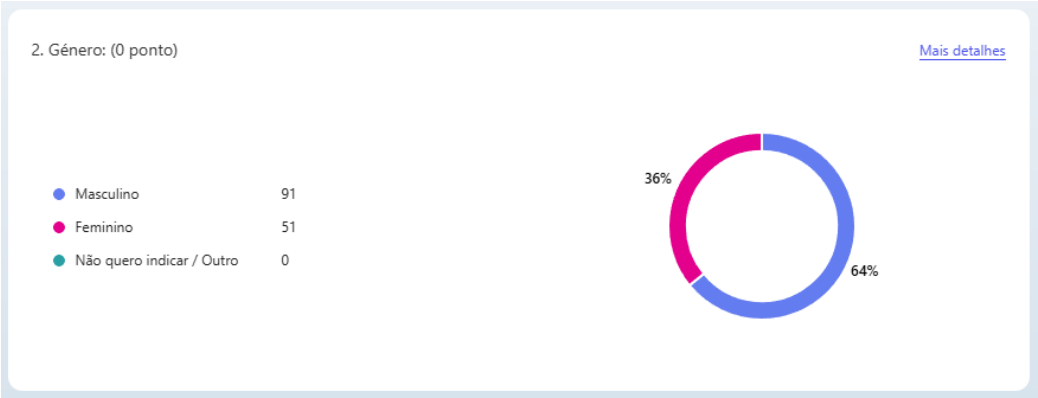


Figura 10 – Número de inquiridos por género

Este dado revela uma maior participação masculina, o que poderá refletir a própria realidade do setor da emergência pré-hospitalar em Portugal, tradicionalmente mais representado por elementos do sexo masculino, sobretudo nas equipas operacionais. Ainda assim, a presença significativa de mulheres entre os inquiridos demonstra uma participação ativa e crescente do género feminino neste contexto profissional, refletindo também uma tendência de maior inclusão e equilíbrio de género nos últimos anos.

Relativamente à faixa etária dos participantes, representada na Figura 11, observa-se uma distribuição relativamente equilibrada, com maior concentração nos escalões intermédios. A maioria dos inquiridos encontra-se entre os 21 e os 50 anos, destacando-se o grupo dos 41 aos 50 anos com 52 seleções (37%), seguido pelos grupos dos 21 aos 30 anos com 40 (28%) e dos 31 aos 40 anos com 31 (22%). Em menor número surgem os participantes com menos de 20 anos (2%) e com mais de 50 anos (11%).

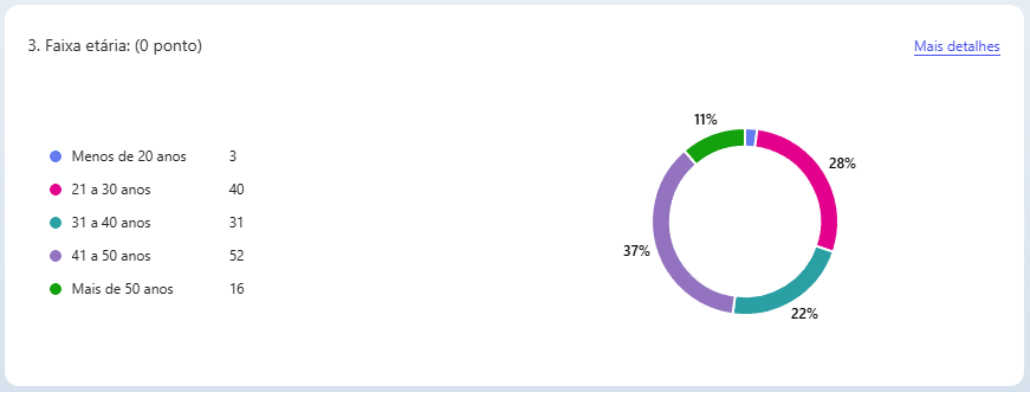


Figura 11 – Número de inquiridos por faixa etária

Esta distribuição etária demonstra uma amostra composta essencialmente por profissionais em plena atividade, com experiência acumulada e, ao mesmo tempo, com

potencial de desenvolvimento e formação contínua. A diversidade etária permite ainda enriquecer os resultados do estudo, ao incorporar diferentes perspetivas e vivências no contexto da emergência pré-hospitalar.

No que respeita ao nível de escolaridade dos participantes, ilustrado na Figura 12, verifica-se que a maioria dos inquiridos possui o 12.º ano de escolaridade ou equivalente, representando 55% da amostra (78 seleções). Seguem-se os participantes com licenciatura (35 seleções, 25%) e, em menor número, os detentores de um curso de especialização tecnológica (CET/CTeSP), com 8% (11 seleções). Apenas 10 participantes (7%) indicaram possuir mestrado, sendo que não se registou qualquer resposta relativa ao doutoramento, nem a níveis de escolaridade inferiores ao 9.º ano.

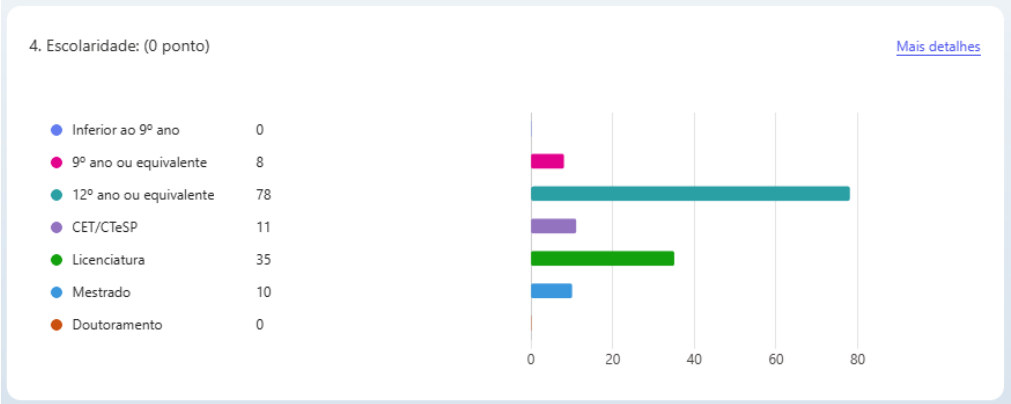


Figura 12 – Número de inquiridos por nível de escolaridade

Estes dados refletem uma amostra maioritariamente composta por profissionais com escolaridade intermédia, o que é coerente com a exigência de formação técnica e certificada associada ao desempenho de funções no contexto da emergência pré-hospitalar. Ainda assim, destaca-se a presença relevante de participantes com formação académica superior, o que poderá traduzir uma maior predisposição para compreender e aplicar os princípios legais associados à proteção de dados.

Relativamente à distribuição geográfica dos inquiridos, representada na Figura 13, constata-se que a maioria dos participantes pertence à região Centro, com 67 respostas, correspondendo a 47% da amostra total. Seguem-se as regiões Lisboa e Vale do Tejo (29 respostas; 20%) e Norte (28 respostas; 20%). Em menor percentagem, o Algarve surge com 10 respostas (7%) e o Alentejo com apenas 8 (6%). Não se registaram respostas oriundas das Regiões Autónomas dos Açores e da Madeira.

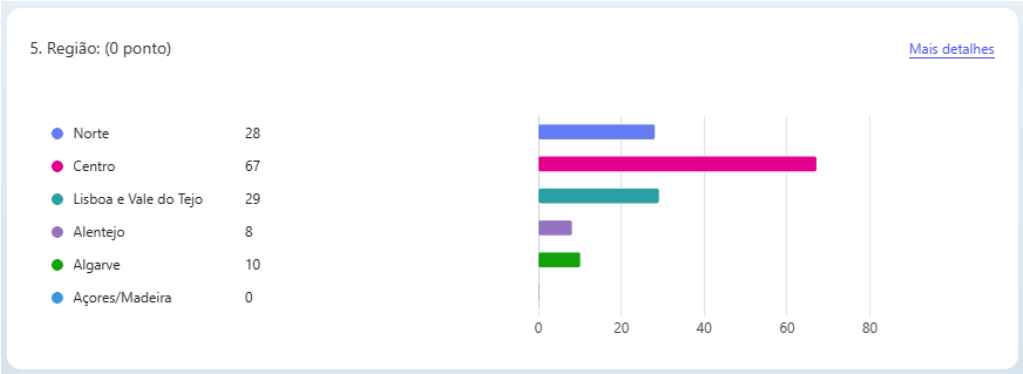


Figura 13 – Número de inquiridos por região

Este padrão pode estar relacionado com a rede de contactos do autor e os canais utilizados para a divulgação do questionário, especialmente junto de instituições e profissionais com atuação mais concentrada na região Centro. Ainda assim, a presença de respostas provenientes de várias zonas do país garante uma certa diversidade territorial, o que contribui para a representatividade do estudo.

No que diz respeito ao tempo de serviço dos participantes, ilustrado na Figura 14, é possível verificar uma distribuição equilibrada entre diferentes níveis de experiência profissional. Destaca-se o facto de a maioria dos participantes possuir uma experiência significativa, com 37 respostas (26%) a indicarem mais de 25 anos de serviço. Segue-se o grupo com menos de 5 anos de experiência, com 35 respostas (25%), o que demonstra também a participação de profissionais mais recentes na atividade. Já os intervalos entre 6 e 10 anos e 11 e 15 anos apresentam, respetivamente, 22 e 23 respostas (15 e 16%), enquanto o intervalo entre 16 e 20 anos foi selecionado por 25 inquiridos (18%).

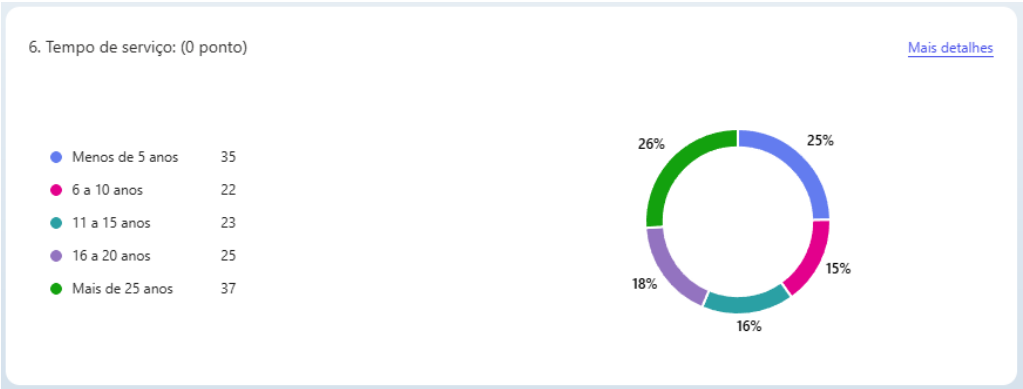


Figura 14 – Número de inquiridos por tempo de serviço

Esta diversidade de tempo de serviço permite aferir que a amostra é composta por profissionais com diferentes níveis de experiência, garantindo uma visão global e transversal

das práticas e perceções no contexto da emergência pré-hospitalar, e contribuindo para uma análise mais representativa e equilibrada do nível de consciencialização existente entre profissionais em diferentes fases da carreira.

Já a análise do vínculo institucional dos profissionais inquiridos, apresentada na Figura 15, revela uma amostra bastante equilibrada entre profissionais e voluntários, com 75 respostas (53%) provenientes de profissionais e 67 (47%) de voluntários.

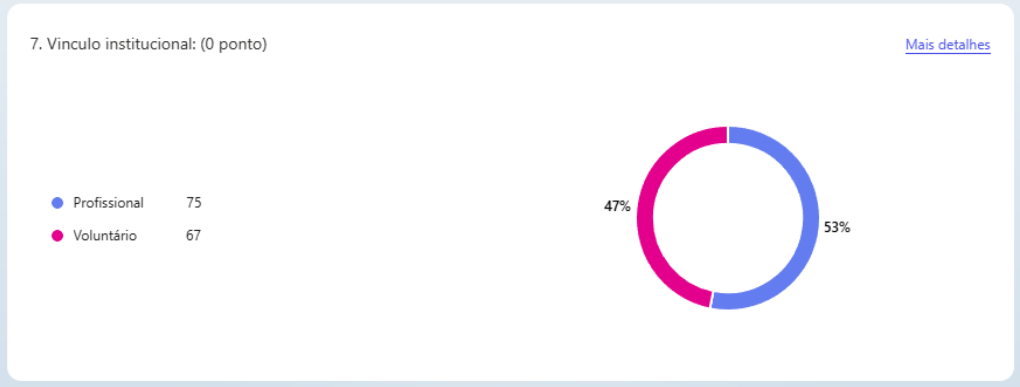


Figura 15 – Número de inquiridos por vínculo profissional

Esta distribuição equitativa permite uma representação justa das duas principais realidades existentes no setor da emergência pré-hospitalar, assegurando que os dados recolhidos reflitam diferentes contextos de atuação, graus de responsabilidade e rotinas operacionais.

Contudo, importa salientar que esta distinção pode, em certos casos, não refletir com total precisão a realidade funcional dos inquiridos. Existem, por exemplo, bombeiros voluntários que exercem funções profissionais no interior das corporações - como operadores de central, socorristas ou motoristas de ambulância - mas que, simultaneamente, continuam a prestar serviços enquanto voluntários. Esta sobreposição de papéis pode introduzir alguma ambiguidade na classificação, influenciando a forma como os próprios participantes interpretam e indicam o seu vínculo institucional no questionário.

Por último, nesta secção, a análise dos resultados relativos à função desempenhada pelos participantes, representada na Figura 16, demonstra que a esmagadora maioria dos inquiridos desempenha funções diretamente ligadas ao socorro e transporte de vítimas em contexto pré-hospitalar. Concretamente, 39 respostas (27%) correspondem a elementos com formação TAT, enquanto 82 participantes (58%) exercem funções como TAS, constituindo este último o grupo mais representativo da amostra.

Registou-se ainda a participação de 1 TEPH e de 4 Enfermeiros, não tendo sido registada qualquer resposta relativa a Médicos. Por fim, 16 participantes (11%) indicaram desempenhar outras funções associadas ao contexto em estudo, designadamente funções de suporte ou de ligação ao socorro, como operadores de comunicações, motoristas, ou outros técnicos com responsabilidades específicas nas respetivas instituições.

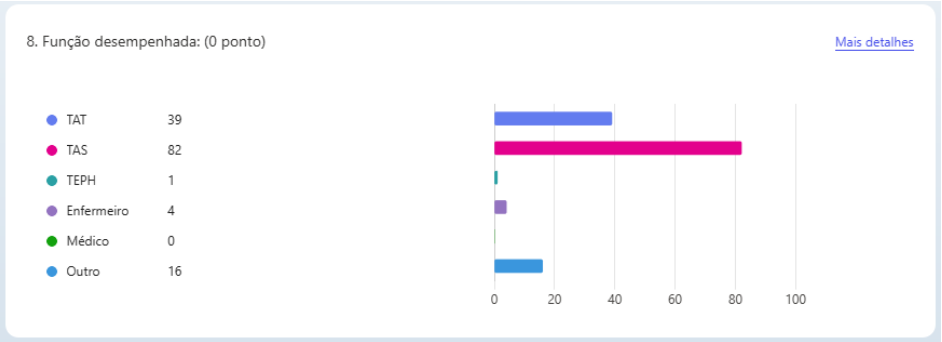


Figura 16 – Número de inquiridos por função desempenhada

Tendo em conta a representatividade dos Corpos de Bombeiros nas ocorrências em contexto de emergência pré-hospitalar, e considerando que os seus elementos possuem, maioritariamente, formações de TAS ou TAT, é expectável que estas funções sejam as que apresentam maior representatividade na amostra recolhida. Este resultado permite, assim, concluir que a amostra está fortemente alinhada com o perfil dos profissionais que mais frequentemente contactam com dados pessoais e sensíveis no terreno, representando uma perspetiva realista das práticas e desafios do socorro pré-hospitalar em Portugal.

A reduzida participação de técnicos de emergência pré-hospitalar, enfermeiros e médicos poderá ser justificada, em parte, pela ausência de resposta, em tempo útil, ao pedido de divulgação oficial do questionário junto do INEM, bem como pela escassa existência de grupos ou canais de partilha dirigidos especificamente a estes perfis nas redes sociais utilizadas para a divulgação.

6.2.2. Perceção sobre a legislação vigente

A segunda secção do questionário inicia-se com a tentativa de aferir o grau de familiaridade dos profissionais com a regulamentação europeia e a legislação nacional relativa à proteção de dados pessoais e sensíveis. Esta pergunta revela-se estratégica, uma vez que permitirá, numa fase posterior, cruzar os resultados obtidos com as respostas dadas nas questões de cenários práticos, permitindo assim aferir se os profissionais possuem efetivamente um conhecimento sólido da legislação ou se apenas acreditam que o detêm.

Os resultados, apresentados na Figura 17, revelam que 67 participantes (47%) afirmam ter conhecimento da legislação em vigor, 12 (8%) indicam desconhecê-la totalmente, e 63 (44%) referem ter apenas um conhecimento parcial.

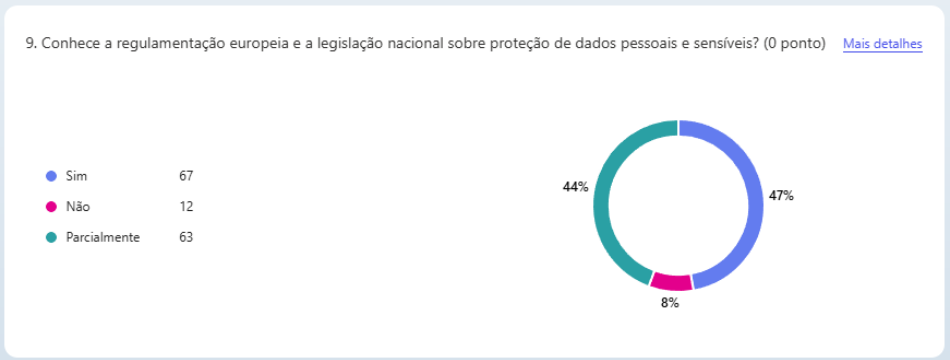


Figura 17 – Número de inquiridos que conhece a legislação europeia e nacional de proteção de dados

Estes dados demonstram que, embora exista uma percentagem relevante de profissionais com alguma familiaridade com o enquadramento legal, quase metade da amostra admite ter apenas uma perceção parcial do mesmo, o que pode indiciar lacunas ao nível da formação e atualização contínua sobre esta matéria essencial.

A segunda questão procurou compreender se os inquiridos já haviam frequentado formação específica na área da proteção de dados pessoais e/ou sensíveis. Dos 143 participantes, 54 (38%) afirmaram ter recebido formação nos últimos cinco anos, 13 (9%) indicaram que essa formação ocorreu há mais de cinco anos, 36 (25%) declararam nunca ter tido qualquer formação, e 39 (27%) referiram que, embora nunca tenham tido formação, gostariam de a frequentar (Figura 18).

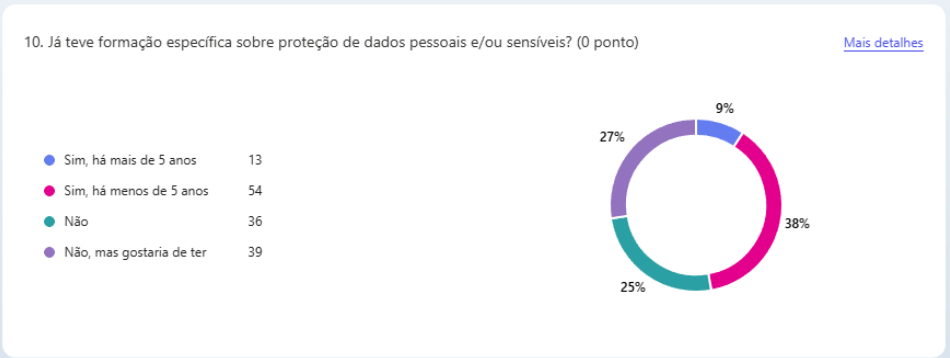


Figura 18 – Número de inquiridos que indicam ter tido, ou não, formação em proteção de dados

Estes resultados assumem particular relevância quando contextualizados com a entrada em vigor do RGPD, em 2018. Considerando a importância que o regulamento assumiu, seria

expectável que a maioria das formações tivesse ocorrido após essa data. A existência de um número significativo de profissionais que nunca recebeu formação (25%) ou que a teve antes da implementação do RGPD (9%) revela a persistência de lacunas na atualização de conhecimentos e na adaptação à legislação vigente. Este dado evidencia a importância de continuar a promover iniciativas formativas regulares, garantindo que os profissionais do setor estejam devidamente capacitados para lidar com dados pessoais e sensíveis no contexto da emergência pré-hospitalar.

Relativamente ao local onde foi obtida a formação em proteção de dados, os resultados demonstram que, dos 67 participantes que afirmaram ter tido formação, a maioria - 32 respostas (48%) - indicou que essa formação foi promovida por uma entidade externa à sua instituição. Por sua vez, 26 respostas (39%) referem que a formação foi disponibilizada internamente pela própria entidade onde o participante exerce funções. Por fim, apenas 9 participantes (13%) afirmaram ter adquirido esses conhecimentos por iniciativa e interesse pessoal (Figura 19).

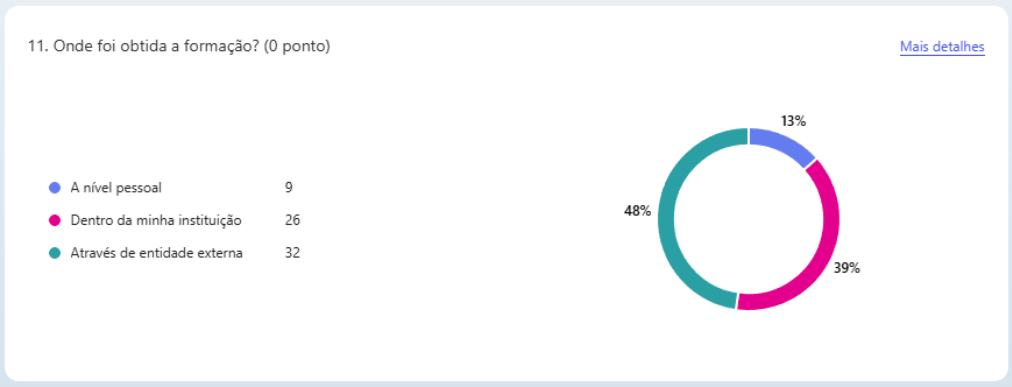


Figura 19 – Número de inquiridos que obtiveram formação, por forma de obtenção

Estes dados permitem concluir que, embora exista um esforço significativo por parte das instituições na formação dos seus profissionais, grande parte da formação obtida resulta de iniciativas externas, provavelmente associadas a ações de formação certificadas ou *workshops*/*webinars* promovidos por entidades especializadas. Este facto demonstra que, apesar das obrigações do RGPD imputarem responsabilidades às entidades empregadoras em matéria de formação (Art. 24.º, nº1 e nº2; Art. 32.º, nº4; e Art. 39.º, nº1, alínea b) do RGPD), ainda subsiste a necessidade de reforçar e sistematizar a formação interna, tornando-a parte integrante e regular dos processos de capacitação dos profissionais de emergência pré-hospitalar.

As próximas e últimas três perguntas desta secção incidem sobre conceitos-base da legislação em matéria de proteção de dados, nomeadamente dados sensíveis, consentimento e princípio da minimização dos dados. Estes temas são, posteriormente, retomados sob a forma de cenários práticos na secção seguinte do questionário. Com esta abordagem paralela pretende-se, mais uma vez, avaliar não só o grau de familiaridade teórica dos profissionais com estes conceitos, mas também aferir se essa perceção corresponde, de facto, a uma correta compreensão e aplicação no terreno.

Nesse sentido, na pergunta evidenciada pela Figura 20 sobre distinção entre dados pessoais de dados sensíveis, os resultados demonstram uma distribuição relativamente equilibrada entre as diferentes opções de resposta. Apenas 58 participantes (41%) afirmaram ter certeza sobre essa distinção, enquanto 61 (43%) admitiram não ter a certeza e 23 (16%) reconheceram que não sabem fazê-lo.

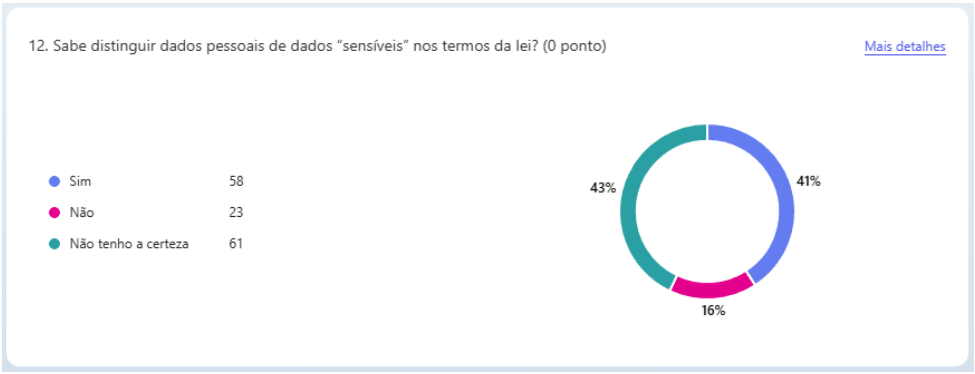


Figura 20 – Número de inquiridos que distingue, ou não, dados pessoais de dados sensíveis

Estes resultados levantam algumas preocupações, tendo em conta que a distinção entre dados pessoais e dados sensíveis é um dos pilares fundamentais da proteção de dados consagrada no RGPD, uma vez que os segundos - como os de saúde, origem étnica, opiniões políticas ou orientação sexual - requerem medidas reforçadas de proteção e restrições acrescidas ao seu tratamento. O facto de mais de metade da amostra (59%) demonstrar incerteza ou desconhecimento em relação a este conceito pode indicar fragilidades importantes na formação ou na consciencialização prática sobre as exigências legais aplicáveis ao contexto de emergência pré-hospitalar.

Na penúltima pergunta da secção - Figura 21, o objetivo passou por perceber se os profissionais estão sensibilizados para o princípio do consentimento, mas também se têm conhecimento das exceções previstas na lei, como é o caso das situações de emergência vital, em que o tratamento de dados é legítimo mesmo sem o consentimento do titular.

Os resultados obtidos demonstram que 83 participantes (58%) consideram que o consentimento é sempre necessário, enquanto 58 (41%) responderam corretamente que nem sempre é necessário, e apenas 1 resposta defendeu que nunca é necessário consentimento.

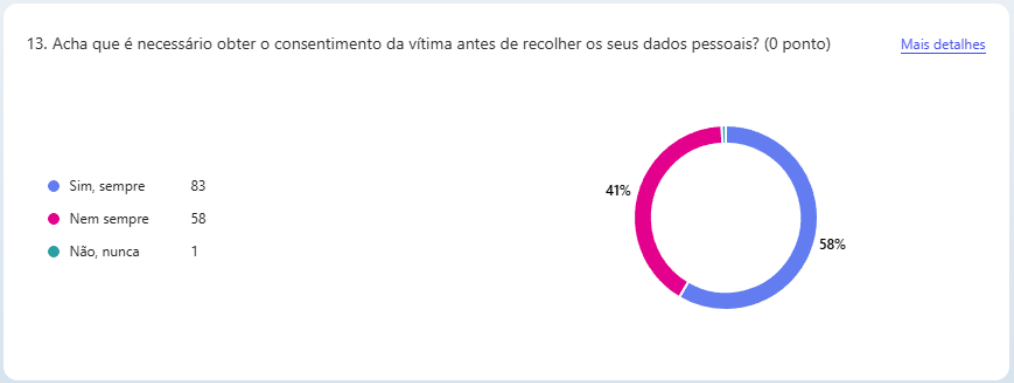


Figura 21 – Número de inquiridos que acha necessário, ou não, obter sempre o consentimento da vítima

Estes resultados revelam que embora a maioria dos profissionais reconheça a importância do consentimento, existe uma percentagem significativa (58%) que, possivelmente por excesso de zelo ou desconhecimento das exceções legais, acredita que este requisito se aplica de forma absoluta em qualquer situação. Este resultado poderá indicar a necessidade de reforçar a formação neste tema, esclarecendo os contextos em que o consentimento é dispensável para garantir o socorro imediato da vítima.

Na última pergunta desta secção pretendeu-se aferir até que ponto os profissionais estão familiarizados com um dos princípios fundamentais consagrados no RGPD. Os resultados obtidos mostram que apenas 42 inquiridos (32%) afirmaram conhecer o conceito e saber o que ele significa. A maioria das respostas ficou dividida entre 55 participantes (39%) que já ouviram falar, mas não sabem exatamente o que é, e 45 respostas (32%) que indicam total desconhecimento do princípio (Figura 22).

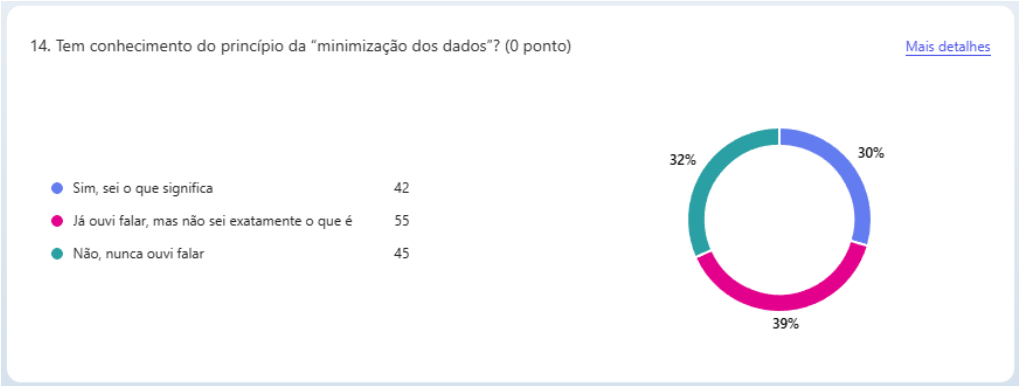


Figura 22 – Número de inquiridos que conhecem, ou não, o princípio da minimização de dados

Este resultado é particularmente relevante, dado que a minimização de dados é um princípio transversal que influencia todas as fases do tratamento de dados pessoais, desde a recolha até à sua conservação. O desconhecimento generalizado da sua definição poderá, portanto, conduzir a práticas excessivas ou inadequadas no terreno, nomeadamente a recolha de informação irrelevante para a prestação de socorro, colocando em risco a privacidade das vítimas. A comparação que se segue com as perguntas de cenários práticos permitirá avaliar até que ponto este desconhecimento teórico se reflete também na prática operacional.

6.2.3. Consciencialização em casos práticos

No iniciar da secção de cenários práticos pretendeu-se avaliar se os profissionais conseguem, na prática, reconhecer corretamente os dados que se inserem nas denominadas categorias especiais de dados pessoais, definidas no Artigo 9.º do RGPD.

Os resultados, ilustrados na Figura 23, revelam que apenas 55 respostas (39%) conseguiram identificar corretamente o único grupo de dados totalmente composto por categorias especiais - Religião, dados relativos à saúde e orientação sexual.

As restantes respostas demonstram alguma confusão por parte dos participantes, sendo que o grupo mais selecionado - Nome completo, morada e número de telefone - foi escolhido por 60 participantes (42%), revelando que muitos profissionais ainda associam, incorretamente, dados pessoais comuns a dados sensíveis, o que pode refletir uma falta de conhecimento técnico preciso.

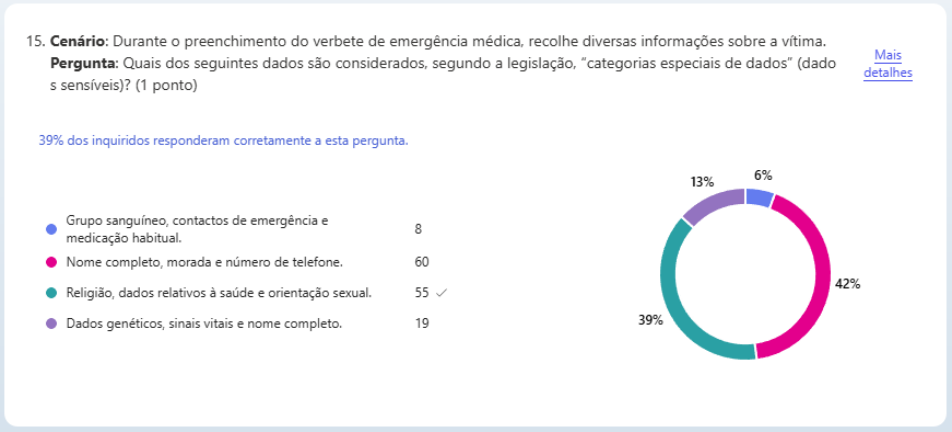


Figura 23 – Distribuição das respostas do cenário de categorias especiais de dados

Estes resultados reforçam a pertinência da análise feita na secção anterior, onde cerca de 69% da amostra admitiu não ter a certeza ou não saber distinguir dados pessoais de dados sensíveis. Assim, confirma-se que a perceção inicial dos profissionais sobre este conceito

fundamental não se traduz, em muitos casos, num conhecimento efetivo e correto da sua aplicação prática.

No segundo cenário prático, ilustrado na Figura 24, procurou-se aferir o procedimento adequado quanto à obtenção de consentimento para a recolha de dados pessoais e sensíveis de uma vítima consciente. A opção correta, foi selecionada por 43 participantes (30%), o que representa uma baixa taxa de acerto, demonstrando alguma confusão por parte dos profissionais sobre as circunstâncias em que o consentimento pode ser dispensado.

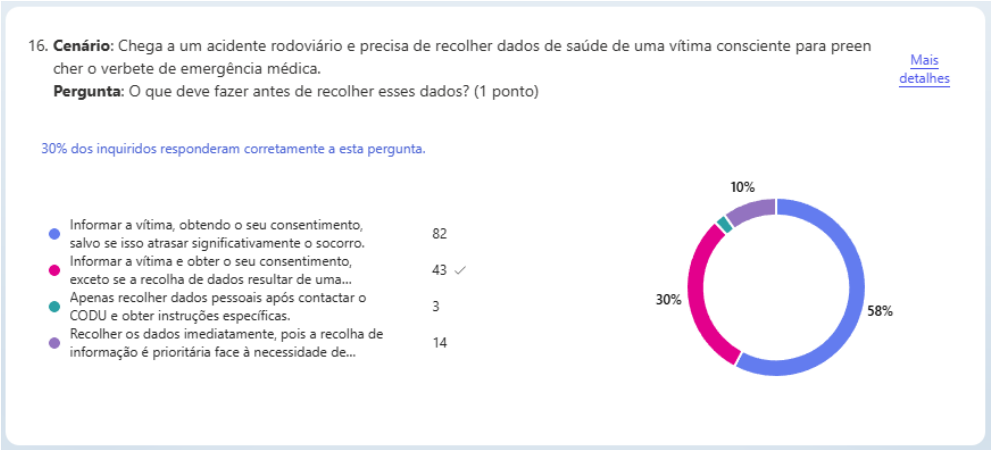


Figura 24 – Distribuição das respostas do cenário de recolha de dados

A escolha maioritária (58%) pela primeira opção era expectável, dado que a diferença entre esta e a opção correta reside numa subtil questão linguística, distinguindo-se entre "informar, obtendo o consentimento" e "informar e obter o consentimento". Apesar de parecerem semelhantes, a primeira expressão transmite incorretamente a ideia de que o simples ato de informar equivale à obtenção de consentimento, o que não é juridicamente válido. O consentimento deve ser uma manifestação clara, livre e informada, distinta do ato de apenas informar.

No cenário seguinte (Figura 25), 40 inquiridos (28%) selecionaram a opção correta, que preconiza a comunicação de informações básicas - como o estado de consciência - respeitando a confidencialidade e avaliando o contexto caso a caso. Apesar de esta orientação não se encontrar expressamente prevista na legislação, representa a opção mais sensata e proporcional, assegurando um equilíbrio entre o dever de sigilo e a necessidade de informação mínima em situações de emergência. A maioria dos inquiridos distribuiu-se pelas restantes opções, que ou permitiam a partilha de informação excessiva, ou bloqueavam por completo qualquer comunicação, sem atender ao contexto específico da ocorrência.

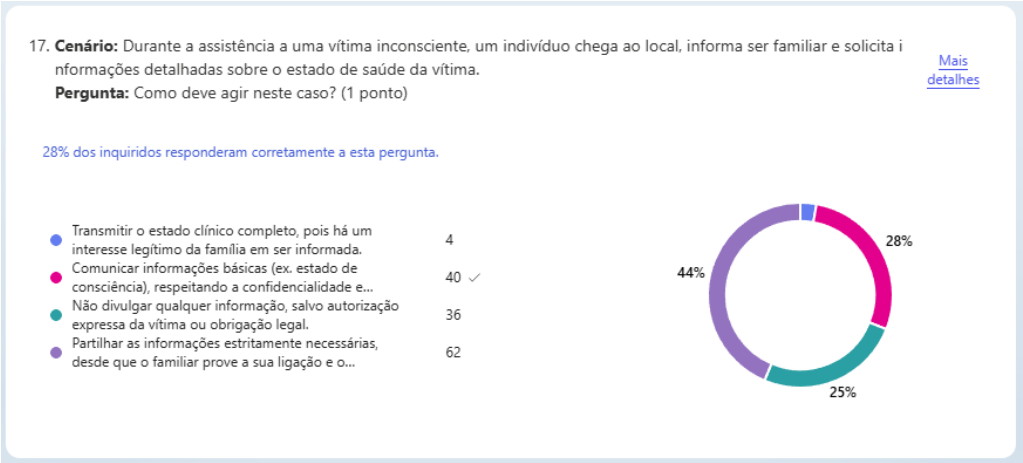


Figura 25 – Distribuição das respostas do cenário de prestação de informação a familiares

Tendo em consideração a opção erradamente mais votada, torna-se importante clarificar que a legislação vigente não prevê qualquer obrigatoriedade de um indivíduo ter de comprovar a sua ligação familiar para que possa obter informações sobre a vítima. Pelo contrário, o dever de sigilo dos profissionais deve ser mantido independentemente dessa alegada ligação, devendo a partilha de informação ser sempre ponderada e limitada ao estritamente necessário, em função do contexto e da proteção da privacidade da vítima.

No cenário seguinte, representado pela Figura 26, os inquiridos foram confrontados com a necessidade de transmitir informações sobre uma vítima ao CODU, tendo à disposição o rádio e o telemóvel de serviço/pessoal. A resposta correta, selecionada por 41% dos participantes (58 seleções), consiste na utilização do telefone, uma vez que este meio de comunicação oferece, regra geral, maior segurança e confidencialidade dos dados transmitidos, reduzindo a possibilidade de escutas não autorizadas em canais abertos.

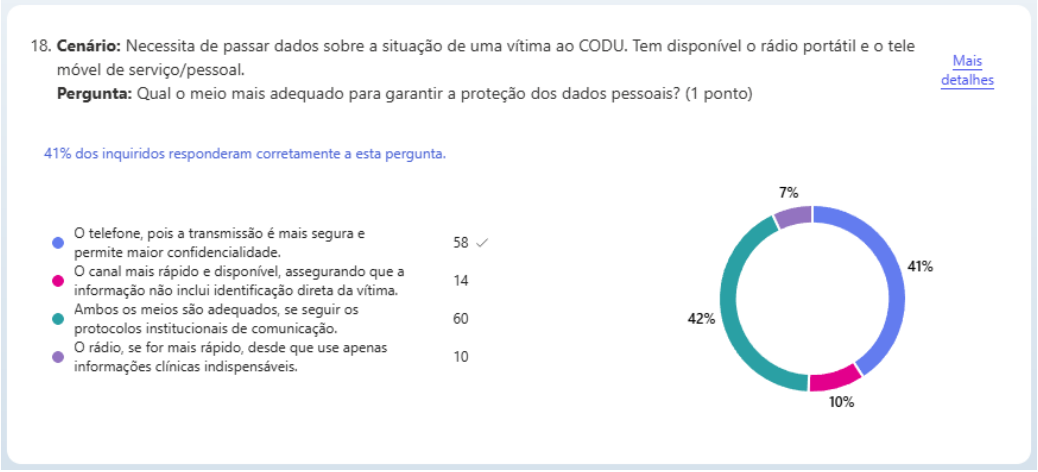


Figura 26 – Distribuição das respostas do cenário de meio de comunicação mais adequado

As restantes opções obtiveram distribuições bastante altas, demonstrando que uma parte significativa da amostra considera que a escolha do meio de comunicação deve depender da urgência ou dos protocolos institucionais existentes. Apesar dessa visão ser válida em determinados contextos operacionais, importa reforçar que, sempre que estejam em causa dados pessoais ou sensíveis, o meio que oferece maior privacidade e segurança deve ser privilegiado - salvo situações de força maior em que o tempo de resposta seja determinante.

Na questão ilustrada pela Figura 27, pretendia-se aferir o conhecimento dos participantes quanto ao destino correto a dar às anotações informais realizadas durante a ocorrência, após estas terem cumprido a sua finalidade.

A resposta correta, escolhida por 61% dos inquiridos (87 respostas), consiste na destruição ou eliminação imediata dessas anotações, uma vez que os dados recolhidos de forma auxiliar não devem ser armazenados para além do tempo estritamente necessário ao cumprimento da finalidade para a qual foram recolhidos, conforme previsto no princípio da limitação da conservação dos dados.

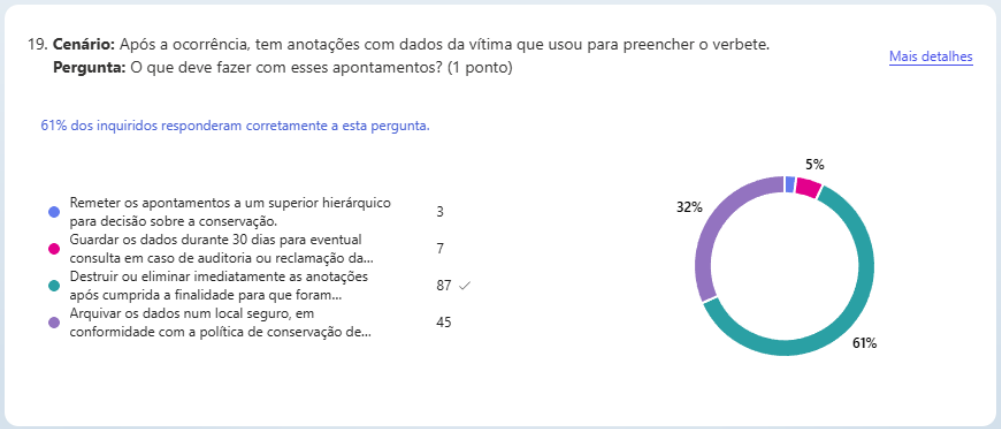


Figura 27 – Distribuição das respostas do cenário de destruição de apontamentos

Apesar de a maioria ter identificado corretamente esta prática, destaca-se que 32% dos participantes optaram por arquivar as anotações durante um determinado período, o que demonstra que ainda subsistem algumas dúvidas sobre este procedimento. Tal situação poderá decorrer da existência de orientações internas divergentes entre instituições ou da perceção de que guardar apontamentos poderá prevenir eventuais reclamações ou auditorias.

Este resultado reforça a necessidade de clarificação e uniformização de procedimentos institucionais no que diz respeito ao armazenamento e destruição de dados pessoais recolhidos informalmente durante a atuação no terreno.

No cenário ilustrado pela Figura 28, onde uma vítima consciente questiona o profissional de emergência sobre o motivo da recolha dos seus dados pessoais e clínicos, pretende-se avaliar se este conhece a sua obrigação legal de prestar informações transparentes relativamente à justificação do tratamento desses dados.

Nesta pergunta, 113 inquiridos (80%) identificaram corretamente que, mesmo em contexto de emergência, é obrigatório informar a vítima sobre o enquadramento do tratamento, nomeadamente a sua finalidade, os destinatários dos dados, o prazo de conservação e os restantes direitos consagrados na legislação.

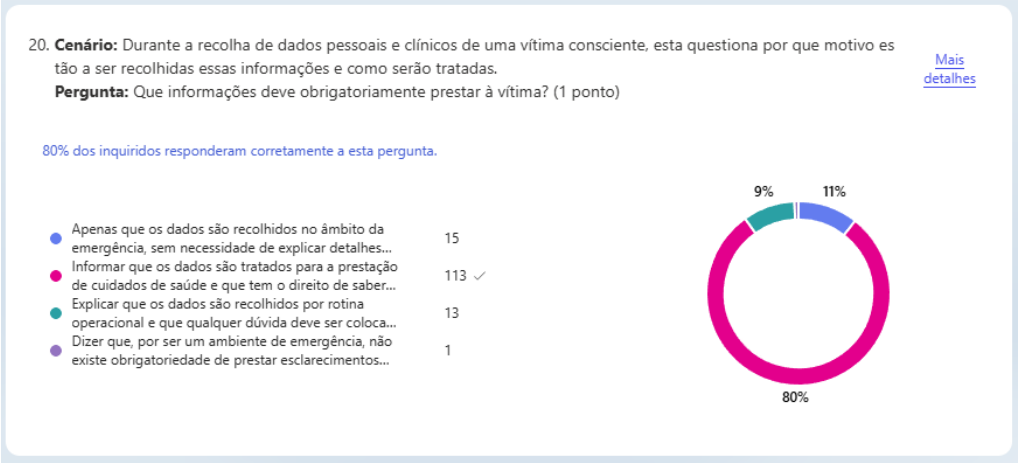


Figura 28 – Distribuição das respostas do cenário de informações a prestar à vítima

Contudo, importa destacar que os restantes 20% das respostas ainda defende abordagens mais simplificadas ou evasivas, o que poderá, em contexto real, comprometer os direitos da vítima enquanto titular dos dados.

Estes resultados, ainda que bastante positivos, sublinham ainda alguma necessidade de reforçar a formação dos profissionais nesta área, garantindo que os deveres de informação são respeitados, mesmo em situações de pressão operacional.

No cenário seguinte, o profissional é notificado pela Comissão Nacional de Proteção de Dados (CNPD) para apresentar prova de que obteve o consentimento da vítima para o tratamento de dados recolhidos durante o socorro. Perante esta situação, apenas 29 inquiridos (20%) selecionaram a escolha certa a tomar (Figura 29).

A resposta correta estabelece que deve ser apresentado o verbete de emergência ou outro registo formal onde conste, de forma expressa, a anotação de que o consentimento foi solicitado e obtido. Este procedimento está alinhado com o princípio da responsabilidade do

responsável pelo tratamento (artigo 5.º, n.º 2, do RGPD), que exige não só o cumprimento, mas também a capacidade de demonstrar conformidade com os princípios aplicáveis.

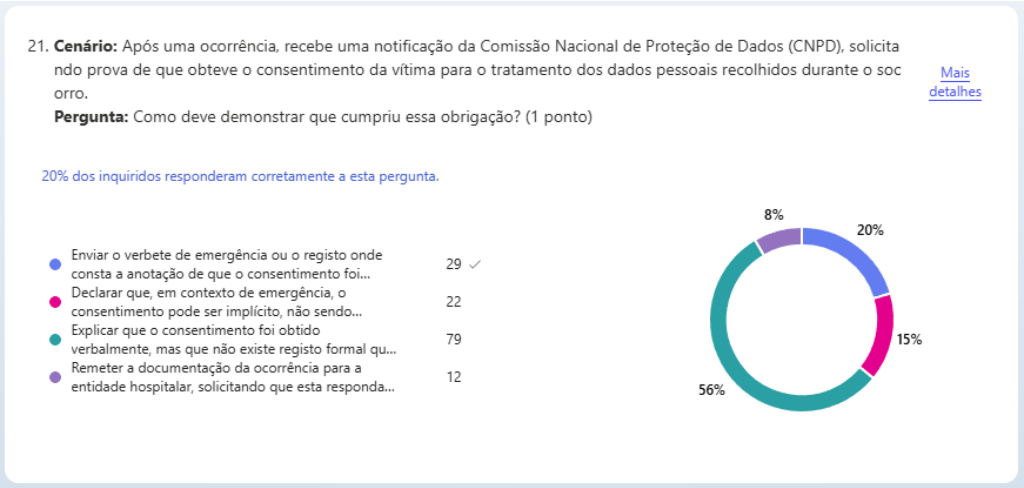


Figura 29 – Distribuição das respostas do cenário de prova do consentimento

O facto de 80% dos participantes terem escolhido respostas incorretas - baseadas em justificações como o caráter verbal do consentimento (56%) ou a inexistência de documentação por se tratar de uma emergência (15%) - demonstra uma fragilidade significativa no entendimento das obrigações legais associadas à prova do consentimento. Como tal, reforça-se a necessidade de se adotarem mecanismos mais claros de registo e rastreabilidade nas instituições, bem como ações formativas sobre este dever.

Já na questão que aborda a possibilidade de remoção do consentimento por parte da vítima após o seu fornecimento, 43% dos inquiridos selecionaram corretamente a opção que esclarece que a vítima tem o direito de retirar o consentimento a qualquer momento.

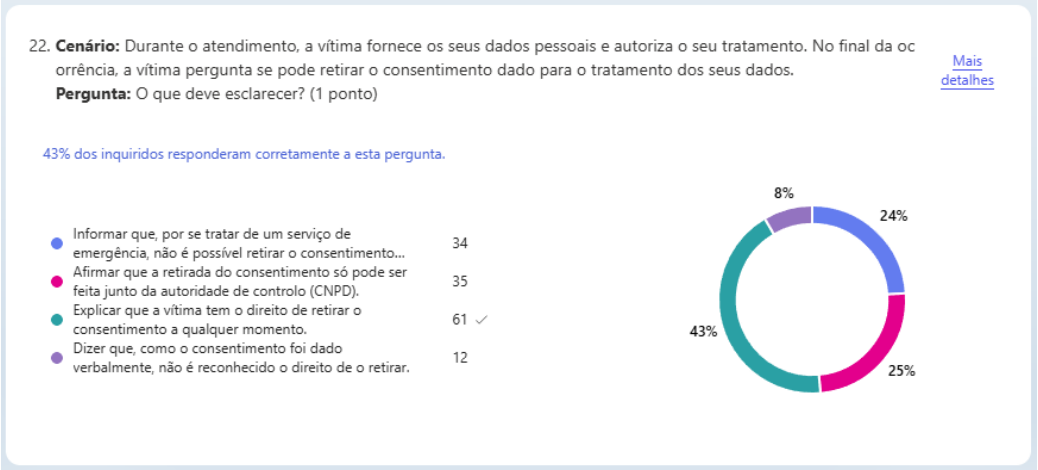


Figura 30 – Distribuição das respostas do cenário da remoção de consentimento

Este direito encontra-se consagrado no RGPD, o qual determina que a remoção do consentimento não compromete a licitude do tratamento efetuado até esse momento. Importa, por isso, que os profissionais de emergência estejam preparados para informar adequadamente a vítima sempre que este pedido seja realizado.

Apesar disso, a maioria dos participantes (57%) considerou incorretamente que o consentimento, uma vez dado, não poderia ser retirado (24%) ou que seria necessário contactar a CNPD para o efeito (25%). Este resultado evidencia a necessidade de reforçar o conhecimento prático dos profissionais sobre os direitos dos titulares dos dados, assegurando o cumprimento da legislação e uma adequada comunicação com as vítimas no contexto do socorro pré-hospitalar.

Relativamente à atuação dos profissionais perante a solicitação de informações por parte de um jornalista no local de uma ocorrência (Figura 31), 42% dos inquiridos (59 respostas) selecionaram corretamente a opção que indica que apenas se deve divulgar informações como o número de vítimas e o tipo de ocorrência, sem partilhar qualquer dado pessoal ou relativo ao estado de saúde das vítimas envolvidas.

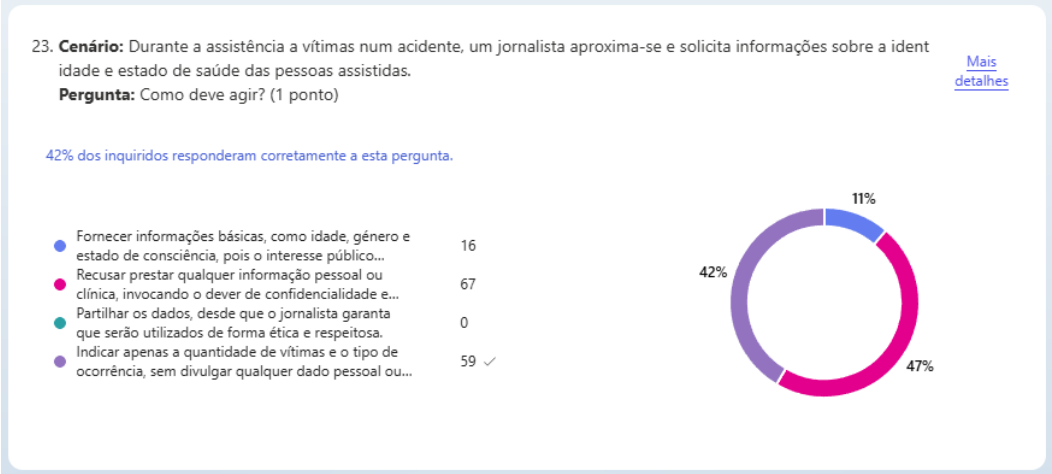


Figura 31 – Distribuição das respostas do cenário do comportamento perante um jornalista

Por outro lado, um total de 67 inquiridos (47%) acredita que a atitude mais adequada passa por recusar prestar qualquer informação, invocando o dever de confidencialidade. Este resultado revela um equívoco frequente, dado que os jornalistas, enquanto agentes de comunicação social, têm direito à liberdade de expressão e de informação (Art. 85.º RGPD). O dever de confidencialidade dos profissionais de emergência não os isenta de fornecer informações gerais e objetivas sobre o cenário da ocorrência, desde que essas informações não coloquem em causa a privacidade das vítimas envolvidas.

Deste modo, aconselha-se que os profissionais de emergência procurem informar-se adequadamente sobre os direitos consagrados na legislação relativamente ao acesso à informação por parte de jornalistas, bem como no âmbito de atividades com fins académicos, artísticos ou literários, garantindo assim uma atuação mais consciente e alinhada com as disposições legais em vigor.

Por fim, a análise dos resultados do último cenário, visível na Figura 32 e relativo à prestação de informações a agentes de autoridade, demonstra que 80 inquiridos (56%) selecionaram corretamente a opção que indica que devem fornecer a esses profissionais os dados pessoais e clínicos estritamente necessários para a realização do auto de ocorrência.

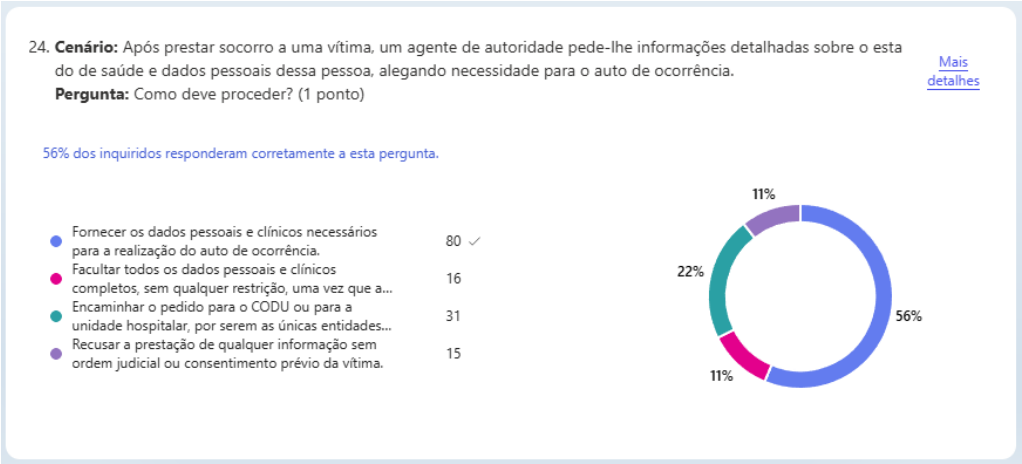


Figura 32 – Distribuição das respostas do cenário do comportamento perante a autoridade

Este positivo resultado demonstra um bom nível de conhecimento quanto à obrigação legal de colaboração com as autoridades, prevista na legislação nacional, nomeadamente no artigo 6.º do RGPD, que prevê a legitimidade do tratamento de dados sempre que este decorra de uma obrigação legal.

Os profissionais que selecionaram as restantes opções devem, perante estas situações, refletir sobre o facto de que estes agentes de autoridade estão também obrigados ao dever de sigilo profissional, pelo que a partilha de dados pessoais e clínicos, quando solicitada no âmbito das suas funções legais, não compromete a proteção da privacidade da vítima, desde que se limite às informações estritamente necessárias e adequadas ao objetivo do pedido. Importa, por isso, reforçar o conhecimento dos profissionais de emergência sobre estas obrigações, evitando interpretações incorretas que possam comprometer a adequada colaboração com as autoridades e a eficiência do socorro prestado.

Com base na análise global das respostas obtidas nas questões baseadas em cenários práticos, é possível calcular que a taxa média de erro foi de aproximadamente 56%, o que revela um dado preocupante. Apesar de se tratar de profissionais com experiência direta no socorro pré-hospitalar e contacto regular com dados pessoais e sensíveis, mais de metade não conseguiu aplicar corretamente os princípios legais em situações reais simuladas.

Este resultado evidencia uma lacuna significativa entre o conhecimento teórico declarado nas secções anteriores e a sua aplicação prática, o que reforça a ideia de que a perceção sobre o domínio da legislação nem sempre corresponde à realidade. Questões como a identificação de categorias especiais de dados (taxa de erro de 61%), a prestação de informações aos familiares (taxa de erro de 72%), a demonstração de obtenção de consentimento (taxa de erro de 80%) e a relação com jornalistas (taxa de erro de 58%) demonstraram ser especialmente desafiantes para muitos dos inquiridos, o que pode colocar em risco tanto a privacidade das vítimas como a segurança jurídica dos próprios profissionais.

6.2.4. Implicações e desafios

A análise das respostas relativas à questão dos principais desafios na aplicação da legislação sobre proteção de dados em contexto pré-hospitalar encontra-se representada na Figura 33. Visualizando a mesma, é possível destacar um conjunto de dificuldades frequentemente percecionadas pelos profissionais, sendo que algumas delas refletem diretamente os problemas identificados e discutidos ao longo deste trabalho.

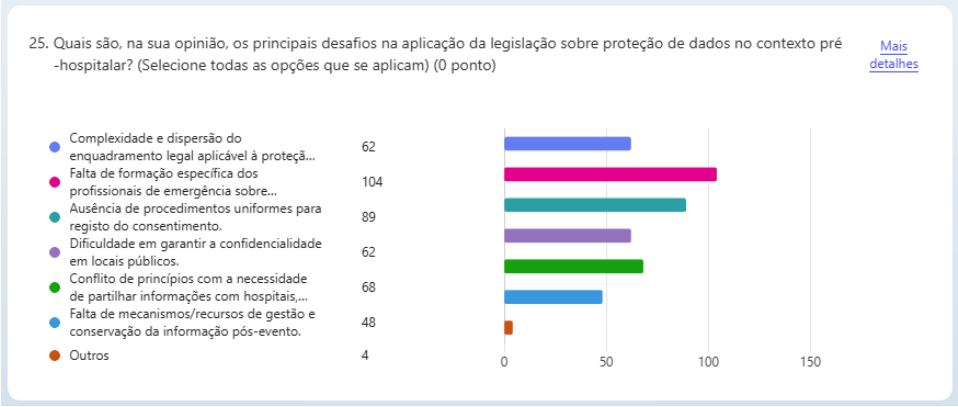


Figura 33 – Distribuição das respostas sobre os principais desafios na aplicação da legislação

O desafio mais votado - indicado por 104 inquiridos - prende-se com a falta de formação específica dos profissionais de emergência sobre proteção de dados. Este resultado não é surpreendente, tendo em conta os dados previamente analisados nas secções anteriores, que

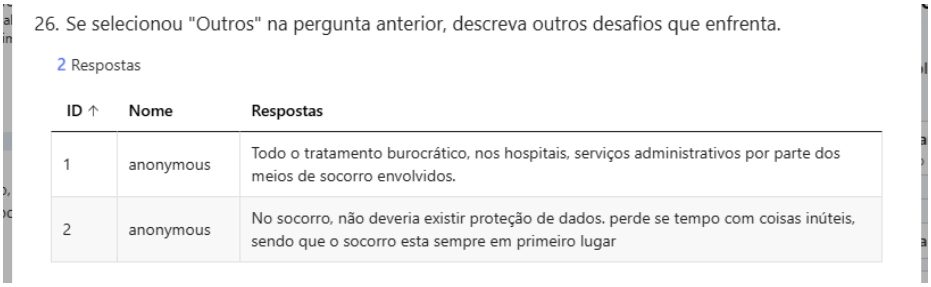
já demonstravam que uma parte significativa da amostra nunca teve contacto com formação adequada sobre o tema. Este fator representa um risco importante, visto que, sem conhecimento técnico e legal apropriado, torna-se mais difícil garantir o cumprimento das obrigações impostas pela regulamentação e legislação vigente.

Em segundo lugar, foi apontada por 89 inquiridos a ausência de procedimentos uniformes para o registo do consentimento. Este desafio mostra-se particularmente relevante no contexto pré-hospitalar, onde a recolha do consentimento da vítima, quando aplicável, ocorre muitas vezes de forma verbal e em ambiente de urgência. A inexistência de orientações claras ou de ferramentas específicas para registo seguro deste consentimento pode originar dificuldades acrescidas para os profissionais e colocar em causa a prova do cumprimento legal.

Além disso, importa dar especial destaque ao desafio da complexidade e dispersão do enquadramento legal aplicável à proteção de dados de saúde, indicado por 62 participantes. Esta perceção demonstra que a legislação atualmente em vigor é, efetivamente, vasta e por vezes difícil de compreender, justificando a realização do presente trabalho, que pretende, justamente, contribuir para mitigar esta dificuldade.

Todas as restantes opções, que serão exploradas em maior detalhe no capítulo seguinte, foram de igual modo amplamente selecionadas, demonstrando que os desafios sentidos no terreno são variados e abrangem diferentes dimensões do processo de tratamento de dados. Este resultado evidencia que a proteção de dados em contexto pré-hospitalar exige uma abordagem integrada e multidisciplinar, capaz de dar resposta a diferentes realidades e dificuldades operacionais vividas pelos profissionais no desempenho das suas funções.

Relativamente aos inquiridos que selecionaram a opção “Outros”, destaca-se a opinião geral de que todo o tratamento de dados realizado durante a ocorrência é um procedimento burocrático demorado e exigente que pode colocar em causa a prestação do socorro à vítima.



26. Se selecionou "Outros" na pergunta anterior, descreva outros desafios que enfrenta.

2 Respostas

ID ↑	Nome	Respostas
1	anonymous	Todo o tratamento burocrático, nos hospitais, serviços administrativos por parte dos meios de socorro envolvidos.
2	anonymous	No socorro, não deveria existir proteção de dados. perde se tempo com coisas inúteis, sendo que o socorro esta sempre em primeiro lugar

Figura 34 – Desafios adicionais identificados pelos inquiridos

6.2.5. Sugestões de melhorias

Na última secção do questionário, os resultados relativos às sugestões de melhoria (Figura 35) indicam de forma clara as principais necessidades sentidas pelos profissionais no terreno para promover um maior nível de conformidade com a legislação de proteção de dados em contexto pré-hospitalar.

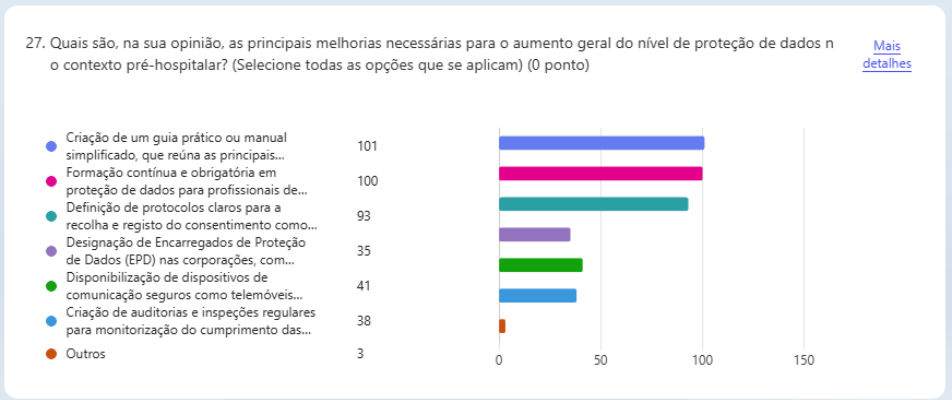


Figura 35 – Distribuição das respostas sobre as principais soluções para combater os desafios

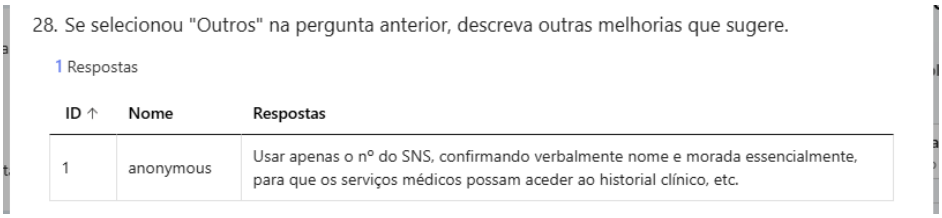
A medida mais votada - a criação de um guia prático ou manual simplificado, que reúna as principais normas de proteção de dados aplicáveis à emergência pré-hospitalar - obteve 101 respostas, evidenciando a necessidade de tornar o enquadramento legal mais acessível e compreensível para os profissionais. Esta preferência reforça a pertinência e utilidade deste próprio trabalho, que procurou exatamente sistematizar e clarificar esse conjunto normativo, oferecendo uma visão mais direta, prática e adaptada ao terreno.

Com um número igualmente elevado de respostas (100), surge a formação contínua e obrigatória em proteção de dados, revelando a consciência generalizada da importância da capacitação dos profissionais nesta matéria. Estes resultados vêm também confirmar a perceção anteriormente evidenciada nos desafios, nomeadamente a reconhecida falta de formação específica, o que reforça a urgência na implementação de programas formativos regulares, adaptados às realidades operacionais das equipas de socorro.

A terceira melhoria mais selecionada, com 93 votos, prende-se com a definição de protocolos claros para a recolha e registo do consentimento, sugerindo, por exemplo, a inclusão de um campo específico nos verbetes de emergência médica. Esta proposta destaca a necessidade de garantir maior uniformidade neste processo, assegurando que os profissionais saibam exatamente como e quando documentar o consentimento das vítimas, cumprindo assim os requisitos legais e protegendo-se de eventuais responsabilidades futuras.

Para além das três melhorias mais votadas, importa referir que as restantes opções de resposta foram igualmente alvo de uma expressiva adesão por parte dos inquiridos, ainda que com cerca de metade do apoio obtido pelas propostas anteriormente analisadas. Este facto demonstra que, apesar de existirem prioridades claras na opinião dos participantes, todas as soluções apresentadas são reconhecidas como relevantes para o aumento do nível de proteção de dados no contexto pré-hospitalar.

Relativamente à opção "Outros", importa destacar que apenas um dos participantes apresentou uma sugestão concreta, referindo que considera adequado que, sempre que possível, se utilize exclusivamente o número de utente do Serviço Nacional de Saúde (SNS), confirmando verbalmente apenas o nome e a morada da vítima, de modo a permitir que os serviços hospitalares acedam de imediato ao historial clínico da vítima (Figura 36).



28. Se selecionou "Outros" na pergunta anterior, descreva outras melhorias que sugere.

1 Respostas

ID ↑	Nome	Respostas
1	anonymous	Usar apenas o nº do SNS, confirmando verbalmente nome e morada essencialmente, para que os serviços médicos possam aceder ao historial clínico, etc.

Figura 36 – Soluções e melhorias adicionais identificadas pelos inquiridos

Esta prática já corresponde à metodologia habitualmente utilizada no socorro em Portugal, pelo que se entende que esta sugestão visa reforçar e incentivar a manutenção desta abordagem, reconhecendo a sua eficácia e adequação ao contexto operativo.

6.3. Análise comparativa de resultados

Para além da análise geral dos resultados obtidos em cada pergunta do questionário, revelou-se igualmente relevante aprofundar a relação entre os dados sociodemográficos dos participantes e o seu desempenho na secção dedicada aos cenários práticos. Esta abordagem permite não só enriquecer a compreensão global do nível de consciencialização da amostra, como também identificar eventuais padrões ou disparidades associadas a determinadas variáveis, como o vínculo institucional, a formação ou o tempo de serviço.

Nesse sentido, recorrendo novamente ao ficheiro Excel exportado diretamente da plataforma de recolha de dados (Apêndice D – Transcrição integral das respostas recolhidas de todos os participantes), iniciou-se o processo de atribuição de cotações às perguntas de cenários práticos, com o objetivo de, posteriormente, calcular a taxa de acerto individual de

cada participante. Assim, foi atribuída a pontuação de 1 valor por cada resposta correta, até ao máximo de 10 pontos possíveis.

De seguida, algumas operações de limpeza de dados foram realizadas, nomeadamente a eliminação de colunas não relevantes para a presente análise, como algumas células em branco ou campos automáticos de *feedback* não preenchidos. Por fim, construiu-se uma tabela dinâmica com base na amostra validada, configurando-se as variáveis sociodemográficas como linhas e a pontuação média total como valor de referência.

Através desta estrutura, tornou-se possível desenvolver uma análise comparativa clara e sistematizada entre diferentes grupos de participantes, cujos resultados se detalham nos subcapítulos que se seguem.

6.3.1. Desempenho por género e faixa etária

Analisar o desempenho por género em articulação com a faixa etária permite compreender de forma mais aprofundada o impacto que fatores como a experiência, a formação recente e as dinâmicas socioprofissionais podem ter no nível de conhecimento prático sobre proteção de dados, oferecendo uma visão mais rica do perfil dos profissionais que integram o sistema de emergência pré-hospitalar.

Nesse sentido, a tabela representada pela Figura 37, revela diferenças interessantes ao nível do desempenho nas questões práticas do questionário.

Género e faixa etária	Média de acerto (em 10)
Feminino	**4,51**
21 a 30 anos	4,91
31 a 40 anos	4,80
41 a 50 anos	3,75
Mais de 50 anos	2,50
Masculino	**4,34**
21 a 30 anos	4,44
31 a 40 anos	4,50
41 a 50 anos	4,28
Mais de 50 anos	3,79
Menos de 20 anos	6,33

Figura 37 – Desempenho dos inquiridos por género e faixa etária

A análise destes dados demonstra que o género feminino registou uma pontuação média global de 4,51 pontos, ligeiramente superior à média do género masculino, que se fixou nos 4,34 pontos. No entanto, ao observar os dados segmentados por faixa etária, verifica-se que entre as mulheres a pontuação tende a decrescer significativamente com o avançar da idade:

enquanto os grupos dos 21 aos 30 anos (4,91) e dos 31 aos 40 anos (4,80) apresentam valores elevados, as médias caem para 3,75 na faixa dos 41 aos 50 anos e para apenas 2,50 no grupo com mais de 50 anos.

No caso dos participantes do sexo masculino, os valores mantêm-se mais estáveis entre os 21 e os 50 anos, com médias que variam entre 4,28 e 4,50 pontos. Apenas na faixa acima dos 50 anos se observa, novamente, uma quebra mais visível, com uma média de 3,79 pontos.

De destacar ainda o grupo com menos de 20 anos, que, embora represente uma amostra reduzida (3 participantes), registou a média mais elevada de todas (6,33 pontos). Este dado pode indicar uma maior atualidade da formação recebida, maior exposição recente ao tema ou, possivelmente, uma maior sensibilidade geracional para as questões da privacidade e da proteção de dados.

De forma geral, esta análise demonstra que os participantes mais jovens tendem a apresentar melhores resultados, reforçando a importância de assegurar formação contínua ao longo da carreira. Além disso, as quebras observadas nas faixas etárias mais avançadas, especialmente no grupo feminino, poderão evidenciar a necessidade de estratégias mais eficazes de atualização normativa junto destes profissionais.

6.3.2. Desempenho por escolaridade

A análise do desempenho médio por nível de escolaridade permite aferir a relação entre o grau académico dos participantes e o seu conhecimento prático sobre proteção de dados no contexto da emergência pré-hospitalar. Numa perspetiva geral, os resultados, ilustrados pela Figura 38, demonstram uma tendência de melhoria do desempenho à medida que o nível de escolaridade aumenta, embora com algumas variações relevantes.

Nível de escolaridade	Média de acerto (em 10)
12º ano ou equivalente	4,18
9º ano ou equivalente	4,13
CET/CTeSP	5,45
Licenciatura	4,49
Mestrado	4,90

Figura 38 – Desempenho dos inquiridos por nível de escolaridade

Os participantes com CET/CteSP apresentam a média mais elevada (5,45), destacando-se dos restantes grupos, o que poderá refletir a forte componente prática e técnica destes cursos, frequentemente direcionados para áreas operacionais como a saúde ou a proteção

civil. Seguem-se os profissionais com mestrado, com uma média de 4,90, valor também significativo e que revela um bom domínio dos princípios abordados. A licenciatura surge com uma média intermédia de 4,49, ligeiramente superior à média global.

Já os inquiridos com o 12.º ano ou com o 9.º ano ou equivalente registam os valores mais baixos (4,18 e 4,13, respetivamente), ainda que não distantes dos restantes, o que pode indicar que a experiência prática ou a formação interna têm, em alguns casos, maior impacto que o percurso académico formal.

Em suma, embora os dados apontem para uma ligeira correlação positiva entre escolaridade e desempenho, verifica-se que a formação técnica e específica poderá ter um peso maior do que o grau académico tradicional neste tipo de conhecimentos.

6.3.3. Desempenho por região

A análise da média de acerto por região geográfica permite perceber se existem disparidades no nível de conhecimento prático sobre proteção de dados entre profissionais de diferentes zonas do país. Os resultados, ilustrados pela Figura 39, revelam diferenças pouco acentuadas, mas ainda assim significativas para efeitos interpretativos.

Região	Média de acerto (em 10)	Moda
Alentejo	4,63	5,00
Algarve	4,70	4,00
Centro	4,15	4,00
Lisboa e Vale do Tejo	4,69	5,00
Norte	4,54	3,00

Figura 39 – Desempenho dos inquiridos por região geográfica

A região do Algarve apresenta a média mais elevada, com 4,70 em 10, logo seguida de Lisboa e Vale do Tejo (4,69) e do Alentejo (4,63), todas com desempenhos acima da média geral (4,37). A região Norte apresenta uma média de 4,54, igualmente positiva, embora ligeiramente inferior às anteriores. Já o Centro regista a média mais baixa da amostra (4,15).

No entanto, ao analisar-se a moda - ou seja, o valor de pontuação mais frequentemente - observa-se que tanto o Centro como o Algarve têm como moda o valor 4. Isto significa que, apesar de o Algarve apresentar a média mais alta da amostra e o Centro a mais baixa, o valor mais comum em ambas as regiões foi o mesmo. Esta aparente contradição explica-se pelo número de respostas recolhidas em cada região: enquanto o Centro teve um volume elevado de participantes (67), o Algarve contou apenas com 10. Assim, no caso do Centro,

mesmo que muitos participantes tenham 4 pontos totais, a presença de um número significativo de respostas com valores mais baixos reduziu substancialmente a média. Já no Algarve, com um número menor de inquiridos e uma distribuição mais concentrada em valores altos, a média permaneceu elevada.

Apesar de todas as regiões apresentarem médias dentro de um intervalo próximo, estas diferenças - incluindo as observadas na moda - sugerem que poderá ser benéfico adaptar estratégias de formação e divulgação consoante o contexto regional, promovendo maior homogeneidade no cumprimento das normas de proteção de dados no âmbito pré-hospitalar.

6.3.4. Desempenho por tempo de serviço

O tempo de serviço, enquanto indicador da experiência adquirida no terreno, constitui uma variável particularmente relevante na análise da consciencialização prática dos profissionais. A avaliação dos resultados em função desta variável permite, assim, aferir se a experiência acumulada ao longo dos anos se traduz numa maior capacidade de aplicar corretamente os princípios da legislação de proteção de dados em contexto real. No entanto, os dados obtidos revelam uma tendência algo contrária ao que seria de esperar à partida.

Através da análise da Figura 40, é possível perceber que os profissionais com menos de 5 anos de serviço registam a melhor média de acerto, com 5,09 em 10, indicando um nível de conhecimento prático superior ao dos restantes grupos. Este resultado poderá refletir a influência de formações mais recentes, maior familiaridade com os regulamentos atuais e uma maior sensibilidade ao tema por parte das novas gerações de profissionais.

Tempo de serviço	Média de acerto (em 10)
11 a 15 anos	4,13
16 a 20 anos	4,56
6 a 10 anos	4,32
Mais de 25 anos	3,86
Menos de 5 anos	5,09

Figura 40 – Desempenho dos inquiridos por tempo de serviço

Já os profissionais com entre 16 e 20 anos de experiência apresentam a segunda melhor média (4,56), seguidos pelo grupo com 6 a 10 anos de serviço (4,32). As médias mais baixas pertencem aos profissionais com mais de 25 anos de serviço (3,86) e aos que têm entre 11 e 15 anos (4,13), o que poderá demonstrar alguma desatualização normativa ou ausência de formação contínua ao longo da carreira.

Ainda relativamente ao tempo de serviço, verifica-se, através da Figura 41, um padrão preocupante quanto à perceção e ao conhecimento efetivo sobre a legislação de proteção de dados. Entre os profissionais com mais de 25 anos de serviço, os que afirmaram não ter conhecimentos sobre a legislação registaram uma pontuação média bastante baixa (2,83 em 10). Contudo, mesmo entre aqueles que declararam ter uma boa perceção sobre o tema, a média não ultrapassou os 4,5 pontos - menos de metade da pontuação total possível.

Tempo de serviço e perceção sobre a legislação	Média de acerto (em 10)
Mais de 25 anos	**3,86**
Não	2,83
Parcialmente	3,86
Sim	4,50
Menos de 5 anos	**5,09**
Não	4,00
Parcialmente	5,36
Sim	5,06

Figura 41 – Perceção dos inquiridos sobre a legislação por tempo de serviço

Curiosamente, entre os profissionais com menos de 5 anos de serviço, o padrão repete-se: embora os resultados sejam ligeiramente superiores, continua a observar-se uma discrepância entre a perceção de conhecimento e o desempenho real no questionário.

Assim, estes dados demonstram que, independentemente da experiência acumulada, muitos profissionais acreditam possuir um bom entendimento das normas legais, mas os seus resultados efetivos sugerem o contrário. Independentemente do tempo de serviço, tal evidência sublinha a importância de ações formativas mais objetivas, que permitam alinhar a perceção com o conhecimento real e garantir a aplicação correta da legislação no contexto pré-hospitalar.

6.3.5. Desempenho por vínculo institucional e função

As últimas variáveis consideradas na análise comparativa são o vínculo institucional e a função ou formação desempenhada, permitindo cruzar dois aspetos determinantes: o tipo de ligação à entidade de emergência (profissional ou voluntária) e o nível de responsabilidade ou qualificação funcional. Esta abordagem possibilita compreender em que medida diferentes perfis operacionais influenciam o desempenho no que diz respeito à aplicação prática da legislação de proteção de dados.

Os resultados, ilustrados pela Figura 42, demonstram alguma consistência entre profissionais e voluntários no geral, com médias de acerto muito próximas: 4,41 nos

profissionais e 4,39 nos voluntários. No entanto, quando o vínculo é desagregado por função, observam-se variações relevantes. No grupo dos profissionais, destacam-se os TAT (4,83) e os profissionais com funções classificadas como "Outro" (4,50), enquanto os TAS registam um desempenho ligeiramente inferior (4,26). O único TEPH participante obteve a pontuação máxima (9,00), o que, embora estatisticamente pouco representativo, traduz um elevado domínio técnico da matéria.

Vínculo institucional e função/formação	Média de acerto (em 10)
Profissional	**4,41**
Enfermeiro	5,00
Outro	4,50
TAS	4,26
TAT	4,83
TEPH	9,00
Voluntário	**4,39**
Enfermeiro	2,50
Outro	3,38
TAS	4,63
TAT	4,58

Figura 42 – Desempenho dos inquiridos por vínculo institucional e função

Já no grupo dos voluntários, os TAS e TAT revelam desempenhos equilibrados (4,63 e 4,58, respetivamente), e superiores aos voluntários que se identificaram com a categoria "Outro" (3,38). De notar ainda o resultado mais baixo do grupo de enfermeiros voluntários (2,50), que sobressai comparativamente aos resultados dos enfermeiros com vínculo profissional. Esta diferença significativa, ainda que apenas expressa pela participação de 4 únicos inquiridos, poderá estar relacionada com o acesso desigual a formação específica e contínua, sendo mais frequente entre enfermeiros profissionais, que estão integrados em instituições de saúde com protocolos e recursos dedicados à proteção de dados, ao contrário dos voluntários, que podem não beneficiar do mesmo nível de acompanhamento e capacitação.

Em suma, estes dados reforçam a importância de continuar a investir na formação prática de todos os intervenientes, independentemente do vínculo institucional, com especial foco nas funções que, apesar de operacionais, podem não ter beneficiado de formação formal suficiente para esta área.

7. Discussão

Concluída a recolha, apresentação e análise dos resultados, torna-se essencial avançar para uma reflexão crítica que permita interpretar, de forma aprofundada, os dados obtidos à luz do conhecimento científico já existente e das dinâmicas reais do contexto pré-hospitalar. A discussão constitui, por isso, uma etapa fundamental no desenvolvimento do presente trabalho, permitindo contextualizar os resultados, compreender as suas implicações e extrair conclusões relevantes para a prática profissional. Só através desta articulação será possível aferir a verdadeira dimensão dos desafios existentes e traçar caminhos para o reforço da proteção de dados no contexto da emergência pré-hospitalar.

A análise estatística descritiva dos dados recolhidos permitiu obter uma visão abrangente sobre o grau de conhecimento e perceção de um conjunto de profissionais relativamente ao tratamento e proteção de dados pessoais e sensíveis. Com uma amostra total de 143 participantes, oriundos de diferentes regiões, com distintos níveis de formação, tempo de serviço e vínculos institucionais, procurou-se refletir a realidade do setor em toda a sua diversidade.

Apesar da participação expressiva e representativa, os dados obtidos evidenciam fragilidades significativas no domínio do conhecimento prático da legislação em vigor. A pontuação média obtida nas questões de cenários práticos - aquelas que mais diretamente avaliam a aplicação concreta dos princípios legais em contextos reais de emergência - foi de 4.4 valores em 10, o que corresponde a uma taxa média de erro de aproximadamente 56%.

Este resultado revela um claro nível insuficiente de conhecimento sobre o tema por parte dos profissionais inquiridos, particularmente no que diz respeito à interpretação e aplicação das normas em situações práticas do dia a dia. Mesmo em domínios que à partida se assumiriam como básicos - como a partilha de informações com familiares, o consentimento em contexto de emergência, ou a destruição de dados após o cumprimento da sua finalidade -, as respostas incorretas superaram as expectativas pré-existentes por parte do autor.

Neste contexto, importa refletir de forma crítica sobre estes resultados, relacionando-os com a literatura existente, as dificuldades específicas do contexto pré-hospitalar e, por fim, apresentar recomendações concretas para os profissionais e para as entidades responsáveis pelo seu enquadramento e formação.

7.1. Interpretação dos resultados em relação à literatura

O primeiro aspeto a ser debatido relaciona-se com a articulação entre os resultados obtidos no caso de estudo e as conclusões identificadas na revisão da literatura. Esta comparação é particularmente relevante uma vez que permite compreender em que medida as perceções e práticas dos profissionais refletem as conclusões já publicadas em estudos anteriores, bem como identificar pontos de convergência ou lacunas ainda existentes entre aquilo que já foi investigado e a realidade atual no terreno.

Numa perspetiva geral, é possível constatar que os dados obtidos através do caso de estudo permitiram confirmar e, em muitos aspetos, reforçar as conclusões previamente identificadas na revisão da literatura. Tal como já referido, a baixa pontuação média nas perguntas de cenários práticos revela vulnerabilidades preocupantes no conhecimento e na aplicação de bases de proteção de dados por parte das equipas de socorro. Este resultado corrobora aquilo que diversos estudos já apontavam, relativamente à existência de falhas significativas na formação dos profissionais de saúde em matéria de proteção de dados, sobretudo em contextos fora do ambiente hospitalar (Tinto, 2018), (Koskimies *et al.*, 2020), (Yeng *et al.*, 2019).

A literatura analisada demonstrou também um foco claro e recorrente no RGPD, compreendendo-se essa centralização pela abrangência que o regulamento assume em grande parte das normas legais aplicáveis (Carvalho, 2022), (Nunes, 2019), (Tinto, 2018). No entanto, também sublinha a necessidade de atenção a contextos específicos, como o pré-hospitalar, onde a natureza imprevisível e urgente das ocorrências coloca desafios particulares (Koskimies *et al.*, 2020), (Geiderman *et al.*, 2006), (Moskop *et al.*, 2005), (Erbay, 2014). Tal como se verificou nas respostas aos cenários práticos, a implementação de princípios como o consentimento informado, a minimização de dados ou o dever de confidencialidade em contexto de emergência levanta dúvidas frequentes, com taxas de erro muito expressivas por parte dos participantes.

A dificuldade de adaptação à legislação, apontada como um desafio comum na literatura, foi também altamente identificada pelos próprios inquiridos, nomeadamente através das respostas sobre os principais obstáculos enfrentados no terreno (Carvalho, 2022). Muitos profissionais relataram incerteza quanto aos procedimentos a adotar em determinadas situações, refletindo uma aplicação pouco clara dos princípios legais, o que confirma a necessidade de investimento em mais medidas de apoio e orientação.

Nesta sequência, destaca-se igualmente a necessidade de governança estruturada, apontada tanto pela literatura como pelo presente caso de estudo (Carvalho, 2022), (Mitra *et al.*, 2023). A criação de políticas internas mais claras, a definição de protocolos de consentimento e a existência de supervisão ativa por parte de encarregados de proteção de dados (DPOs) foram identificadas como medidas essenciais para promover a conformidade e a segurança no tratamento de dados pessoais e sensíveis no contexto de socorro.

A revisão dos trabalhos relacionados concluiu ainda a existência de lacunas no conhecimento como um entrave persistente à boa prática (Tinto, 2018), (Koskimies *et al.*, 2020), (Yeng *et al.*, 2019). Esta perceção é confirmada pelos dados do inquérito, onde uma parte significativa dos profissionais refere não ter tido formação específica sobre proteção de dados ou ter apenas um conhecimento parcial dos conceitos envolvidos. Este desfasamento entre o que é legalmente exigido e o que é efetivamente compreendido por quem atua no terreno revela-se também particularmente problemático.

Por fim, a escassez de literatura sobre o tema, anteriormente referida por diversos autores como Koskimies *et al*. (2020), é confirmada não apenas pela análise de fontes realizada neste trabalho, mas também pelas respostas dos próprios participantes, que identificaram como um dos desafios a existência de pouca informação clara, prática e direcionada ao setor da emergência pré-hospitalar. Esta ausência de conteúdos específicos contribui para o desenvolvimento de hábitos desajustados ou inseguros e justifica a necessidade de criação de materiais orientadores que respondam diretamente às dúvidas dos profissionais.

Em suma, os resultados obtidos não só validam as principais conclusões da literatura explorada, como reforçam a urgência de transformar essas constatações em medidas concretas de formação, normalização e apoio prático no terreno.

7.2. Dificuldades para a prática pré-hospitalar

A aplicação das normas de proteção de dados em contexto pré-hospitalar levanta um conjunto de dificuldades concretas que merecem análise detalhada. Tendo em conta os resultados do estudo e a realidade do terreno, torna-se essencial refletir sobre os principais obstáculos sentidos pelos profissionais de emergência no cumprimento da legislação em vigor. Foi para esse efeito que se incluiu no questionário a secção dedicada à identificação dos maiores desafios associados à implementação operacional do enquadramento legal, cujas

opções foram previamente definidas com base na revisão da literatura, na legislação analisada e na experiência do autor enquanto bombeiro voluntário.

A complexidade e dispersão do enquadramento legal aplicável à proteção de dados representa, de facto, um dos maiores entraves à aplicação coerente da legislação no terreno. A ausência de um documento único e dirigido especificamente à realidade da emergência pré-hospitalar obriga os profissionais a recorrerem a múltiplas fontes - entre regulamentos, diretivas e leis nacionais - o que se torna impraticável num ambiente operacional onde o tempo é limitado e as decisões têm de ser imediatas. Esta dispersão legislativa, aliada à linguagem jurídica frequentemente técnica e distante da prática, acaba por afastar os profissionais do verdadeiro conteúdo normativo, dificultando muitas vezes a sua assimilação e aplicação.

Uma vez mais, a falta de formação específica é igualmente sentida de forma muito clara. No contexto, por exemplo, dos corpos de bombeiros são raras, ou até mesmo inexistentes, as formações direcionadas exclusivamente à proteção de dados, e mesmo quando ocorrem, tendem a ser genéricas, superficiais ou descontextualizadas. Esta realidade contrasta com a responsabilidade legal imposta a quem recolhe e trata dados sensíveis, gerando um descompasso perigoso entre a exigência legal e a preparação efetiva dos profissionais.

A ausência de procedimentos uniformes para registo do consentimento revela-se um outro problema relevante e frequentemente ignorado. A inexistência de orientações claras sobre como e onde registar adequadamente o consentimento da vítima - seja verbal, escrito ou presumido - faz com que esta etapa fundamental da proteção de dados seja muitas vezes negligenciada ou mal compreendida. O atual modelo de verbete de emergência, por exemplo, não contempla qualquer campo específico destinado ao consentimento, o que compromete o cumprimento do princípio da licitude e dificulta eventuais auditorias ou pedidos de prova por parte da CNPD.

A dificuldade em garantir a confidencialidade em locais públicos é uma consequência direta das condições imprevisíveis e expostas em que decorrem muitas ocorrências. É comum que vítimas sejam abordadas em plena via pública, cercadas por familiares, amigos ou curiosos, o que torna a partilha de informações particularmente sensível. Neste contexto, a necessidade de comunicar com a vítima, o CODU ou outros meios envolvidos, sem comprometer dados pessoais, é um desafio constante, que exige atenção redobrada e capacidade de julgamento ético e legal.

Também o conflito entre os princípios legais e a necessidade de partilhar informações com hospitais, forças de segurança ou outras entidades, reflete uma dificuldade prática de grande relevância. Os profissionais encontram-se frequentemente num equilíbrio delicado entre cumprir o dever de sigilo e colaborar eficazmente com outras entidades do sistema de emergência. Esta dualidade cria insegurança quanto à quantidade de informação que pode ou deve ser partilhada, gerando, por vezes, decisões contraditórias ou arriscadas.

Por fim, a falta de mecanismos e recursos para a gestão e conservação da informação após a ocorrência é igualmente um desafio que permanece muitas vezes invisível, mas que afeta diretamente a conformidade com os princípios da conservação e da integridade dos dados. A inexistência de orientações claras sobre onde, como e por quanto tempo guardar os documentos gerados durante o socorro - como verbetes ou registos de comunicação - pode comprometer a rastreabilidade do tratamento e dificultar eventuais investigações, auditorias ou pedidos de acesso por parte dos titulares dos dados.

Em suma, embora exista atualmente um enquadramento jurídico relativamente extenso no que diz respeito à proteção de dados, a sua tradução e aplicação prática em contexto de emergência pré-hospitalar continua a levantar desafios significativos. A análise dos resultados do caso de estudo evidenciou a persistência de dúvidas e incertezas por parte dos profissionais, frequentemente causadas por conflitos entre princípios legais, pela ausência de orientações operacionais claras e pela complexidade das situações enfrentadas no terreno.

Perante este cenário, revela-se cada vez mais imperativo adotar medidas concretas de mitigação capazes de atenuar as dificuldades identificadas.

7.3. Recomendações para profissionais e entidades

Com base nos desafios e nas lacunas de conhecimento e procedimentos observadas ao longo deste estudo, importa, por fim, apresentar algumas sugestões de melhoria orientadas para profissionais e entidades, com o intuito de reforçar a proteção de dados no contexto da emergência pré-hospitalar.

A título individual, as equipas devem adotar boas práticas de registo que salvaguardem não apenas a segurança da informação, mas também a sua própria responsabilização legal. Por exemplo, sempre que a recolha de dados sensíveis for realizada com base no consentimento verbal da vítima, recomenda-se que essa autorização seja anotada no campo

de observações do verbete de emergência médica ou iTeams, como forma de documentar o cumprimento das obrigações legais e de mitigar riscos futuros em caso de fiscalização.

Aconselha-se igualmente que os profissionais e as instituições adotem medidas de segurança física, como a guarda dos verbetes preenchidos em armários trancados e reservados apenas a pessoal autorizado, bem como o armazenamento dos equipamentos eletrónicos utilizados em locais seguros dentro das instalações das entidades. Em contexto de transporte, o acesso aos dispositivos iTeams ou similares deve ser limitado e monitorizado, evitando a exposição acidental de dados durante ou após o atendimento.

Adicionalmente, cada profissional deve procurar estar informado sobre os seus direitos e deveres em matéria de proteção de dados. A leitura e consulta de documentos como o presente trabalho, podem servir como ponto de partida para uma compreensão mais clara da legislação aplicável e das boas práticas a adotar. Sendo este estudo um contributo prático e acessível, recomenda-se que seja utilizado como guia introdutório para a reflexão e sensibilização sobre o tema.

No que diz respeito às entidades responsáveis pelo enquadramento e formação destes profissionais, destaca-se a importância de fomentar a realização de formações práticas e específicas, adaptadas ao contexto do socorro. Estas formações devem abordar situações reais, promover o esclarecimento de dúvidas operacionais e consolidar conhecimentos através de simulações e casos de estudo.

Além disso, recomenda-se ainda que as entidades ponderem a disponibilização de dispositivos de comunicação dedicados ao serviço, como telemóveis institucionais protegidos, para a transmissão de dados pessoais, evitando a utilização de equipamentos pessoais e assegurando a existência de canais mais seguros para a partilha de informações sensíveis entre as entidades envolvidas no socorro.

Adicionalmente, recomenda-se ao INEM que considere a introdução de um símbolo ou menção gráfica explícita de "Documento Confidencial", tal como exemplificado pela Figura 43, no canto superior do verbete nacional de socorro. Embora atualmente exista, em rodapé e com reduzida visibilidade, uma indicação de que se trata de dados confidenciais, uma sinalização mais destacada reforçaria a perceção de sigilo por parte de todos os intervenientes no processo, promovendo uma maior consciência quanto à natureza sensível da informação constante no documento e à necessidade do seu manuseamento responsável.

Figura 43 – Sugestão de melhoria ao verbete nacional de socorro

Além disso, sugere-se ainda ao INEM que insira tanto no verbete físico como no iTeams um campo extra onde o socorrista possa declarar a obtenção do consentimento verbal.

Por parte das entidades competentes, sugere-se também a criação e disponibilização de um guia de uso rápido com características semelhantes ao elaborado no Apêndice E do presente trabalho. Este guia, de formato conciso e linguagem acessível, poderá funcionar como um recurso prático de apoio às equipas de socorro, permitindo-lhes relembrar, de forma célere e eficaz, os principais aspetos legais a considerar no decurso de uma ocorrência. Entre os temas a incluir destacam-se o dever de confidencialidade, as condições legais para o tratamento de dados de saúde e os procedimentos adequados para o pedido e registo do consentimento, promovendo assim uma atuação mais informada e juridicamente segura.

Em último caso, as entidades poderão também proteger-se de eventuais responsabilidades jurídicas através da implementação de mecanismos de auditoria e inspeções regulares internas, que permitam verificar o cumprimento das normas de proteção de dados, detetar falhas e corrigi-las atempadamente, demonstrando diligência e compromisso com a privacidade das vítimas.

Por fim, importa também recordar duas dimensões frequentemente negligenciadas no terreno. Em primeiro lugar, a confidencialidade em espaços públicos, que deve ser garantida preferencialmente através da troca de informações em ambientes reservados, como a célula da ambulância, de forma a proteger a privacidade da vítima. Em segundo lugar, o aparente conflito entre o dever de sigilo e a necessidade de colaboração com outras entidades - nomeadamente hospitais ou forças de segurança - deve ser interpretado à luz do princípio de que todos os intervenientes estão, igualmente, sujeitos a obrigações legais de confidencialidade, sendo essa partilha legítima quando necessária e enquadrada na lei.

Assim, estas recomendações representam medidas exequíveis que, se implementadas de forma consistente, espera-se que contribuam significativamente para a melhoria do cumprimento legal e para o reforço da proteção dos dados das vítimas em situações urgentes.

8. Conclusão

O capítulo de conclusão assume um papel determinante na consolidação de qualquer projeto de investigação, na medida em que permite refletir sobre o percurso desenvolvido, sintetizar os resultados alcançados e avaliar o impacto global do trabalho realizado. Para além de proporcionar uma visão estruturada e abrangente dos principais contributos do estudo, este capítulo constitui também uma oportunidade para analisar criticamente as decisões metodológicas, os desafios enfrentados e as soluções encontradas ao longo do processo.

Neste contexto, são agora discutidos, de forma integrada, os resultados obtidos e o valor acrescentado que este projeto representa, quer para o autor, quer para a comunidade académica e profissional na área da proteção de dados em contexto de emergência pré-hospitalar. Serão ainda abordadas as principais limitações encontradas, bem como sugestões de melhoria e propostas para futuras réplicas ou aprofundamentos deste estudo.

Para enquadrar adequadamente esta reflexão final, o capítulo inicia-se com a recapitulação dos objetivos definidos na fase inicial do projeto, permitindo avaliar de forma clara em que medida foram alcançados e qual o grau de cumprimento das metas delineadas.

8.1. Resumo dos objetivos

No início deste projeto, foram estabelecidos diversos objetivos que orientaram todo o processo de investigação, tendo como principal foco garantir o seu cumprimento integral ao longo das diferentes etapas do trabalho. Esses objetivos permitiram estruturar a análise teórica e prática sobre o tratamento e a proteção de dados no contexto da emergência pré-hospitalar, assegurando uma abordagem coerente e alinhada com as necessidades reais do setor.

Os dois primeiros objetivos - explorar os conceitos essenciais associados ao tema e identificar o tipo de dados recolhidos durante operações de emergência, bem como os respetivos métodos de recolha, armazenamento e partilha - foram alcançados no Capítulo 3, dedicado ao enquadramento e caracterização do contexto da emergência pré-hospitalar. Este capítulo permitiu consolidar uma base sólida de compreensão sobre o funcionamento dos serviços de socorro e sobre os tipos de informação frequentemente tratados.

O terceiro objetivo, centrado na análise das obrigações legais impostas por códigos de proteção de dados como o RGPD, no contexto específico da emergência pré-hospitalar, foi cumprido ao longo do Capítulo 4, que tratou com detalhe o enquadramento normativo europeu e nacional, bem como os principais princípios legais aplicáveis.

Já o quarto objetivo - identificar as obrigações legais dos profissionais e os direitos dos titulares dos dados - foi concretizado no Capítulo 5, onde se procurou apresentar, com clareza, as principais obrigações e direitos, através da exemplificação com situações práticas e do cruzamento com os diplomas legais analisados.

Os objetivos quinto, sexto e sétimo, que visavam avaliar o nível de consciencialização dos profissionais, aferir as práticas adotadas no terreno e identificar os principais desafios na aplicação das normas, foram alcançados através da realização do caso de estudo apresentado no Capítulo 6. O questionário desenvolvido e as respetivas respostas obtidas permitiram recolher dados relevantes sobre a realidade vivida pelos profissionais da emergência pré-hospitalar.

Por fim, o oitavo objetivo, que se propunha compreender o impacto e as implicações éticas da legislação para as operações de emergência, foi tratado no Capítulo 7 - Discussão -, mais concretamente no subcapítulo 7.2, onde se analisam os principais obstáculos práticos à implementação das normas legais neste setor de atividade.

Neste sentido, é possível concluir que os objetivos inicialmente delineados foram globalmente atingidos, permitindo uma abordagem completa e coerente ao tema estudado.

8.2. Principais conclusões e contributos

Do desenvolvimento deste projeto emergiram diversos resultados, conclusões e contributos, com impacto tanto ao nível académico e profissional, como pessoal.

Para a comunidade em geral - incluindo civis e profissionais da área da emergência pré-hospitalar - este trabalho representa a criação de um documento único e abrangente que sintetiza o enquadramento normativo relacionado com a proteção de dados neste setor. Esta consolidação legislativa, anteriormente dispersa por diferentes diplomas legais e regulamentos, foi agora apresentada de forma clara, acessível e aplicada, permitindo uma melhor compreensão dos direitos dos titulares dos dados (as vítimas) e das obrigações legais impostas aos profissionais que atuam no terreno. O projeto contribuiu ainda para dar a

conhecer o funcionamento interno dos serviços de socorro e permitiu compreender o grau de consciencialização atual de uma amostra de profissionais relativamente ao tratamento de dados pessoais e sensíveis. Acresce ainda o facto de ter sido possível reunir, através da revisão da literatura, os principais trabalhos já realizados sobre este tema, bem como identificar a sua escassez, reforçando a necessidade de novos estudos neste setor.

No que diz respeito à área científica da proteção de dados no contexto da saúde e do socorro, este trabalho ofereceu um contributo relevante ao abordar uma vertente ainda pouco explorada: a operacionalização dos princípios da legislação em situações de emergência. O estudo procura fornecer uma visão prática e concreta sobre como estas normas podem (e devem) ser aplicadas em contextos altamente sensíveis e dinâmicos, onde o tempo e a informação são fatores críticos. Através do estudo de caso e da análise das respostas obtidas, foram também apresentados dados que poderão servir de base para futuras investigações, políticas de formação ou revisão de procedimentos operacionais no setor da emergência médica.

A nível pessoal, este projeto revelou-se também uma experiência extremamente enriquecedora para o autor. Permitiu aprofundar uma área pouco explorada ao longo do percurso académico - a componente jurídico-legal da proteção de dados - e adquirir conhecimentos que se revelam altamente relevantes tanto para o futuro profissional, na área da Cibersegurança, como também para a prática voluntária enquanto Bombeiro. Esta dualidade entre teoria e prática proporcionou uma visão mais integrada e crítica sobre o tema, deixando o autor mais consciente e preparado para lidar com questões relacionadas com a proteção de dados tanto em situações gerais como em cenários reais de emergência.

8.3. Desafios

Ao longo de todo o trabalho, surgiram diversos desafios que exigiram uma abordagem crítica, persistente e adaptativa. Um dos primeiros e mais significativos relaciona-se com a escassez de bibliografia científica centrada diretamente na intersecção entre proteção de dados e emergência pré-hospitalar. Apesar de existirem muitos trabalhos sobre cada uma das áreas individualmente, os estudos que relacionam ambas são bastante limitados. Este facto obrigou a uma abordagem mais exploratória, exigindo a adaptação de conteúdos de áreas conexas, como a saúde em ambiente hospitalar, e uma interpretação cuidadosa das fontes disponíveis.

Outro aspeto relevante foi a dificuldade em reunir e sistematizar toda a legislação relevante ao tema em estudo. A proteção de dados em contexto de emergência pré-hospitalar encontra-se implicitamente regulada por múltiplos diplomas, tanto a nível europeu como nacional, os quais estão frequentemente dispersos, pouco consolidados e, por vezes, desatualizados. Exigiu-se assim uma análise rigorosa, uma leitura detalhada de cada norma e o esforço de os articular de forma coerente, compreensível e útil para a prática profissional.

A construção do questionário constituiu também um desafio considerável, dada a necessidade de garantir que o instrumento permitia recolher dados relevantes de forma clara, sem induzir em erro ou sugerir respostas corretas, e ao mesmo tempo manter um nível de complexidade adequado para avaliar o verdadeiro conhecimento e perceção dos profissionais. Para isso, o processo passou por várias versões e pela realização de testes com revisores que permitiram validar a estrutura, a linguagem e a pertinência das questões formuladas.

Por fim, um dos desafios transversais a todo o trabalho foi o de traduzir linguagem jurídica e técnica para um discurso acessível, claro e coerente. Ao tratar-se de um tema com uma forte componente normativa, foi fundamental manter o rigor técnico sem comprometer a compreensibilidade do texto, especialmente nas secções destinadas à análise de obrigações e direitos no terreno. Este equilíbrio exigiu um esforço contínuo de revisão e reformulação ao longo de todo o processo de escrita.

8.4. Possíveis limitações

Apesar do esforço desenvolvido para garantir a solidez metodológica e a relevância prática deste estudo, importa reconhecer um conjunto de limitações que poderão ter impacto na generalização e profundidade das conclusões alcançadas.

Em primeiro lugar, salienta-se a inexistência, à data da realização deste trabalho, de um instrumento de recolha de dados previamente validado cientificamente para o contexto específico da proteção de dados em situações de emergência pré-hospitalar. Esta limitação implicou o desenvolvimento autónomo de um questionário, com base em pressupostos teóricos e na experiência prática do autor, o que poderá ter condicionado a robustez do instrumento em termos de fiabilidade e validade.

Em segundo lugar, a amostra utilizada foi de natureza não probabilística e baseada em conveniência, refletindo essencialmente a acessibilidade aos participantes. Esta escolha metodológica, embora justificável em função dos recursos e tempo disponíveis, implica que

os resultados não possam ser generalizados para o universo mais vasto de profissionais de emergência pré-hospitalar em Portugal. Além disso, a amostra revelou-se assimétrica em termos de representação geográfica, experiência profissional e funções desempenhadas, não garantindo uma estratificação adequada dos perfis de resposta.

Também a própria análise dos resultados, apesar de assentar em dados quantitativos recolhidos através de questões objetivas, pode comportar alguma subjetividade, na medida em que a interpretação dos padrões de resposta foi, em diversos casos, influenciada por pressupostos ou hipóteses do autor sobre os motivos subjacentes aos comportamentos ou perceções dos participantes.

Por fim, reconhece-se que o tema da proteção de dados em contexto pré-hospitalar se encontra em constante evolução, quer no plano jurídico, quer no plano técnico-operacional. Assim, as conclusões agora apresentadas devem ser lidas à luz da realidade vigente à data do estudo, podendo necessitar de revisão ou atualização futura, à medida que novas normas, tecnologias ou práticas forem sendo adotadas.

Reconhecer estas limitações não invalida, no entanto, a relevância do trabalho desenvolvido, mas antes reforça a necessidade de investigação adicional, idealmente com amostras mais representativas, instrumentos validados e abordagens metodológicas complementares que contribuam para um entendimento mais abrangente e preciso deste domínio.

8.5. Melhorias e trabalho futuro

É de notar que todo e qualquer trabalho é suscetível de ajustes e aperfeiçoamentos. Durante e após a implementação do projeto, foi possível identificar algumas melhorias que poderão, em versões futuras, aumentar a eficácia, o rigor e a aplicabilidade do trabalho desenvolvido.

Em primeiro lugar, a revisão de literatura poderá, eventualmente, ser refinada. Apesar de ter sido conduzida de forma extensa e minuciosa, é possível que exista algum trabalho complementar, focado em temáticas próximas, que não tenha sido identificado no processo inicial de pesquisa. Um melhor cruzamento entre as conclusões dos diversos estudos poderá agregar valor ao projeto, enriquecendo a fundamentação teórica e permitindo uma comparação mais ampla entre investigações já realizadas.

Uma segunda melhoria prende-se com a estrutura do questionário aplicado. Ainda que este tenha sido cuidadosamente elaborado e validado, a sua versão futura poderá beneficiar de uma organização mais concisa e linguagem objetiva, sem comprometer a profundidade da informação recolhida. Esta otimização poderá potenciar a taxa de resposta e melhorar a experiência do participante.

O alargamento da amostra é também uma melhoria desejável, nomeadamente através de estratégias de divulgação mais abrangentes que permitam chegar a diferentes regiões e a um número mais representativo de profissionais. Paralelamente, a aplicação do questionário em contextos internacionais - mediante tradução e adaptação cultural - abriria portas a uma análise comparativa entre diferentes realidades operacionais e legais, enriquecendo significativamente a discussão e as conclusões do estudo.

Por fim, uma componente inovadora que poderá ser explorada no futuro seria a análise forense digital de plataformas tecnológicas utilizadas no contexto do socorro, como a aplicação iTeams. Este aprofundamento técnico permitiria compreender melhor eventuais vulnerabilidades de segurança e o grau de proteção efetiva dos dados pessoais ali registados, aliando a vertente legal à vertente técnica num contributo multidisciplinar valioso.

Apesar da possibilidade de aperfeiçoamentos, acredita-se que o trabalho realizado cumpriu integralmente os objetivos traçados tanto pelo autor como pela instituição de ensino, contribuindo em diferentes dimensões para a clarificação de um tema ainda pouco explorado, mas de elevada importância na realidade atual da proteção de dados pessoais em contexto de emergência pré-hospitalar.

Referências

Barros, F., Lourenço, J., Ladeira, L., & Ramos, R. (Out. 2019). *ITeams: Manual clínico*. (Consultado em nov. 14, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P. (Aprender INEM): https://aprender.inem.pt/pluginfile.php/1300/mod_resource/content/13/ITEAMS%20manual.pdf

INEM. (Fev. 11, 2024). *Mais de 1.5 milhões de chamadas de emergência atendidas nos CODU do INEM em 2023.* (Consultado em nov. 14, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2024/02/11/mais-de-1-5-milhoes-de-chamadas-de-emergencia-atendidas-nos-codu-do-inem-em-2023/

Morgado, L. (Dez. 27, 2024). *Literature Reviews integrating AI tools*. (Consultado em jan. 20, 2025). Obtido de Repositório Aberto da Universidade Aberta: https://repositorioaberto.uab.pt/entities/publication/17f5ba74-c46d-4aa2-93a8-b8603102d2ea

Carvalho, C. (Mar. 2022). *A Proteção de Dados Pessoais de Saúde*. (Consultado em dez. 10, 2024). Obtido de IC-Online, Instituto Politécnico de Leiria: https://iconline.ipleiria.pt/handle/10400.8/8824

Nunes, G. (Jun. 2019). *O tratamento de dados pessoais de saúde à luz do regulamento geral europeu de proteção de dados pessoais*. (Consultado em dez. 10, 2024). Obtido de Repositório Científico da Universidade de Coimbra: https://estudogeral.sib.uc.pt/handle/10316/89580

SPMS, EPE. (s.d.). *Privacidade da Informação no setor da Saúde*. (Consultado em dez. 30, 2024). Obtido de Ministério da Saúde: https://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

Tinto, A. (Ago. 2018). *Protecção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia.* (Consultado em dez. 10, 2024). Obtido de Repositório Universidade Nova: https://run.unl.pt/handle/10362/58821

Andrade, F., Costa, A., & Novais, P. (2011). *Privacidade e proteção de dados nos cuidados de saúde de Idosos*. (Consultado em jan. 28, 2025). Obtido de Repositorium – Universidade do Minho: https://repositorium.sdum.uminho.pt/handle/1822/15197

INEM, DFEM, DEM, Martins, C., Gala, C., Campos, G., Feu, J., & Lourenço, J. (Mar. 2024). *Curso TAS: Tripulante de Ambulância de Socorro*. (Consultado em nov. 23, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P. (Aprender INEM): https://aprender.inem.pt/pluginfile.php/358741/mod_resource/content/2/MANUAL_TAS_V1_MAR24.pdf

Lima, R. (2021). *RGPD - Regulamento Geral de Proteção de Dados*. (Consultado em Jan. 21, 2025). Obtido de INEM: https://aprender.inem.pt/course/view.php?id=83

Koskimies, E., Koskinen, S., Leino-Kilpi, H., & Suhonen, R. (Set. 5, 2020). *The informational privacy of patients in prehospital emergency care — Integrative literature review*. (Consultado em jan. 15, 2025). Obtido de Research Portal:*University of Turku*: https://research.utu.fi/converis/portal/detail/publication/49029347

Singh, Y., Jaiswal, S., & Kumar, V. (2024). *A Comprehensive Literature Review on Privacy, Security, and Data Management in Healthcare*. (Consultado em jan. 22, 2025). Obtido de IEEExplore: https://ieeexplore.ieee.org/document/10489013

Mitra, A., Gochhait, S., Obaid, A., & Alkhafaji, M. (2023). *A Strategic Data Protection Plan for the Healthcare Industry-A Review*. (Consultado em jan. 22, 2025). Obtido de IEEExplore: https://ieeexplore.ieee.org/document/10192830

Yeng, P., Yang, B., & Snekkenes, E. (2019). *Framework for Healthcare Security Practice Analysis, Modeling and Incentivizatio*n. (Consultado em jan. 23, 2025). Obtido de IEEExplore: https://ieeexplore.ieee.org/document/9006529

Singh, G., Tiwari, D., Goel, P., Vishwakarma, P., Gupto, K., & Verma, A. (2024). *Cybersecurity Challenges In Healthcare Systems*. (Consultado em jan. 23, 2025). Obtido de IEEExplore: https://ieeexplore.ieee.org/document/10593022

Shingari, N., Verma, S., Mago, B., & Javeid, M. (2023). *A review of cybersecurity challenges and recommendations in the healthcare sector*. (Consultado em jan. 23, 2025). Obtido de IEEExplore: https://ieeexplore.ieee.org/document/10111096

Geiderman, J., Moskop, J., & Derse, A. (2006). *Privacy and Confidentiality in Emergency Medicine: Obligations and Challenges*. (Consultado em jan. 24, 2025). Obtido de *ScienceDirect*: https://www.sciencedirect.com/science/article/pii/S0733862706000332

Moskop, J., Marco, C., Larkin, G., Geiderman, J., & Derse, A. (2005). *From Hippocrates to HIPAA: Privacy and confidentiality in Emergency Medicine—Part II: Challenges in the emergency department*. (Consultado em jan. 28, 2025). Obtido de *ScienceDirect*: https://www.sciencedirect.com/science/article/pii/S019606440401282X

Erbay, H. (2014). *Some Ethical Issues in Prehospital Emergency Medicine*. (Consultado em jan. 24, 2025). Obtido de *ScienceDirect*: https://www.sciencedirect.com/science/article/pii/S2452247316300747

Zorab, O., Robinson, M., & Endacott, R. (2015). *Are prehospital treatment or conveyance decisions affected by an ambulance crew's ability to access a patient's health information?* (Consultado em jan. 24, 2025). Obtido de *BMC Emergency Medicine*: https://doi.org/10.1186/s12873-015-0054-1

Koskimies, E., Koskenniemi, J., & Leino-Kilpi, H. (2019). *Patient's informational privacy in prehospital emergency care: Paramedics' perspective*. (Consultado em jan. 26, 2025). Obtido de *Sage Journals*: https://journals.sagepub.com/doi/10.1177/0969733019834977

INEM. (Nov. 23, 2020). *Gestos que salvam! – Quais os Critérios do INEM para Enviar Meios de Socorro.* (Consultado em nov. 22, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2020/11/23/gestos-que-salvam-quais-os-criterios-do-inem-para-enviar-meios-de-socorro-5/

M. Alexandre. (Jun. 20, 2023). Qual a importância do atendimento pré-hospitalar? (Consultado em nov. 22, 2024). Obtido de Hospital Israelita Albert Einstein: https://vidasaudavel.einstein.br/qual-a-importancia-do-atendimento-prehospitalar/

Leitão, F. (Maio, 2022). *Emergência Médica Pré-Hospitalar*. (Consultado em nov. 22, 2024). Obtido de Repositório Aberto da Universidade do Porto: https://repositorio-aberto.up.pt/handle/10216/142169

INEM. (s.d.). *O que é o Sistema Integrado de Emergência Médica (SIEM)?* (Consultado em nov. 22, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.:

https://www.inem.pt/2017/05/26/o-que-e-o-sistema-integrado-de-emergencia-medica-siem/

INEM. (Nov. 22, 2021). *Há 50 anos era criado o Serviço Nacional de Ambulâncias*. (Consultado em nov. 22, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2021/11/22/ha-50-anos-era-criado-o-servico-nacional-de-ambulancias/

Cruz Vermelha Portuguesa. (s.d.). *Breve historial*. (Consultado em nov. 22, 2024). Obtido de Cruz Vermelha Portuguesa: https://www.cruzvermelha.pt/as-nossas-pessoas/breve-historial.html

INEM. (2013). *SIEM: SISTEMA INTEGRADO DE EMERGÊNCIA MÉDICA*. (Consultado em nov. 23, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P. (Aprender INEM): https://aprender.inem.pt/pluginfile.php/110992/mod_resource/content/1/Sistema-Integrado-de-Emergencia-Medica.pdf

INEM. (2024). *Indicadores de Desempenho do INEM*. (Consultado em nov. 25, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://extranet.inem.pt/stats/

INEM. (Nov. 3, 2021). *INEM disponibiliza formação online sobre RGPD para operacionais do SIEM*. (Consultado em nov. 15, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2021/11/03/inem-disponibiliza-formacao-online-sobre-rgpd-para-operacionais-do-siem/

ENB. (Set. 16, 2021) *Webinar: A Proteção de Dados no Sistema Integrado de Emergência Médica (SIEM).* (Consultado em nov. 15, 2024). Obtido de Youtube: https://www.youtube.com/watch?v=W4aEacbwAUU

Valente, M., Catarino, R., Ribeiro, H., Martins, A., Batuca, A., Alves, C., & Rebelo, R. (2012). *O tripulante de Ambulância. Manual TAT*. (Consultado em nov. 27, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/wp-content/uploads/2017/06/O-Tripulante-de-Ambulância.pdf

Martins, C. (Nov. 10, 2017). *O modelo de funcionamento do serviço 112 em Portugal: Actualidade.* (Consultado em nov. 27, 2024). Obtido de Repositório Comum:

https://comum.rcaap.pt/bitstream/10400.26/35123/1/O%20modelo%20de%20funcionamento%20do%20serviço%20112%20em%20Portugal.pdf

INEM. (2023). *Relatório de Atividade do CODU & Meios*. (Consultado em nov. 30, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/wp-content/uploads/2024/07/Relatorio-CODU-e-Meios-2023_-VFF-AprovAss.pdf

INEM. (Nov. 20, 2024). *iTeams® faz 6 anos esta semana*. (Consultado em nov. 30, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2024/11/20/iteams-faz-6-anos-esta-semana/

INEM. (s.d.). *Manual Operacional: iTeams INEM TOOL for EMERGENCY ALERT MEDICAL SYSTEM*. (Consultado em dez. 2, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P. (Aprender INEM): https://aprender.inem.pt/pluginfile.php/145115/mod_resource/content/9/ITEAMS%20MANUAL%20OPERACIONAL.pdf

INEM. (s.d.). *Documentação: Verbete Nacional de Socorro* (Consultado em dez. 4, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/category/documentacao/verbete-nacional-de-socorro/

Rogado, R. (Nov. 28, 2024). *INEM: centro de atendimento voltou a ficar sem sistema informático*. (Consultado em dez. 4, 2024). Obtido de SIC Notícias: https://sicnoticias.pt/pais/2024-11-28-video-inem-centro-de-atendimento-voltou-a-ficar-sem-sistema-informatico-0d69a963

INEM. (s.d.). *Cidadãos: Acesso a Dados sobre Ocorrências*. (Consultado em dez. 6, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/category/cidadaos/acesso-a-dados-sobre-ocorrencias/

INEM. (2017). *Pedido de Acesso a Dados - ocorrências*. (Consultado em dez. 6, 2024). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/wp-content/uploads/2017/06/02.3-Informações-e-ou-documentos-necessários-A-juntar-ao-requerimento.pdf

INEM. (2022). *Política Geral de Segurança da Informação*. (Consultado em jan. 29, 2025). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2022/02/14/politica-geral-de-seguranca-da-informacao/

INEM. (2018). *Política de Privacidade e Proteção de Dados Pessoais do Instituto Nacional de Emergência Médica (INEM)*. (Consultado em jan. 29, 2025). Obtido de Instituto Nacional de Emergência Médica (INEM), I.P.: https://www.inem.pt/2018/06/04/rgpd/

Wikipedia. (Jan. 19, 2024). *Juramento de Hipócrates*. (Consultado em jan. 12, 2025). Obtido de Wikipedia: https://pt.wikipedia.org/wiki/Juramento_de_Hipócrates

Nações Unidas. (s.d.). *Declaração Universal dos Direitos Humanos*. (Consultado em jan. 12, 2025). Obtido de Centro Regional de Informação para a Europa Ocidental: https://unric.org/pt/declaracao-universal-dos-direitos-humanos/

Conselho da Europa. (s.d.). *Convenção Europeia dos Direitos do Homem*. (Consultado em jan. 12, 2025). Obtido de Tribunal Europeu dos Direitos do Homem: https://www.echr.coe.int/documents/d/echr/Convention_POR

Carvalho M., & Lopes P. (Dez. 16, 2019). *Privacidade e Proteção Dados*. (Consultado em jan. 12, 2025). Obtido de Universidade D'Coimbra: https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/privacidade-e-protecao-dados/

Osswald. (Out. 7, 1970). *Data Protection Act.* (Consultado em jan. 12, 2025). Obtido de Gloria González Fuster Blog: https://glgonzalezfuster.blog/history-of-data-protection-an-online-anthology/history-of-data-protection-1970

Conselho da Europa. (Set. 26, 1973). *On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*. (Consultado em Jan. 12, 2025). Obtido de Conselho da Europa: https://rm.coe.int/1680502830

Conselho da Europa. (Set. 20, 1974). *Relative a la protection de la vie privee des personnes physiques vis-a-vis des banques de donnees electroniques dans le secteur public*. (Consultado em jan. 12, 2025). Obtido de Conselho da Europa: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804cd7a9

Wikipedia. (Out. 29, 2024). *Data Act (Sweden)*. (Consultado em jan. 12, 2025). Obtido de Wikipedia: https://en.wikipedia.org/wiki/Data_Act_(Sweden)

Assembleia da República. (Abr. 10, 1976). *Constituição da República Portuguesa - CRP - Artigo 35.º*. (Consultado em jan. 12, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775-49410775

OCDE. (2022). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. (Consultado em jan. 12, 2025). Obtido de: https://dn720002.ca.archive.org/0/items/oecd-legal-0188-en/OECD-LEGAL-0188-en.pdf

Conselho da Europa. (Jan. 28, 1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. (Consultado em jan. 12, 2025). Obtido de Conselho da Europa: https://www.coe.int/en/web/data-protection/convention108-and-protocol

União Europeia. (Out. 24, 1995). *Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046

UNESCO. (2001). *Declaração Universal sobre o Genoma Humano e os Direitos Humanos: da teoria à prática*. (Consultado em jan. 12, 2025). Obtido de UNESCO Digital Library: https://unesdoc.unesco.org/ark:/48223/pf0000122990_por

Assembleia da República. (Out. 26, 1998). *Lei n.º 67/98, de 26 de outubro*. (Consultado em jan. 12, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/67-1998-239857

União Europeia. (Out. 26, 2012). Carta dos Direitos Fundamentais da União Europeia. (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT

União Europeia. (Jul. 12, 2002). *Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção*

da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058

UNESCO. (2004). *Declaração Internacional sobre os Dados Genéticos Humanos*. (Consultado em jan. 12, 2025). Obtido de Biblioteca Virtual em Saúde: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_inter_dados_genericos.pdf

Assembleia da República. (Ago. 18, 2004). *Lei n.º 41/2004, de 18 de agosto*. (Consultado em jan. 12, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710

Assembleia da República. (Jan. 26, 2005). *Lei n.º 12/2005, de 26 de janeiro*. (Consultado em jan. 12, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/12-2005-624463

União Europeia. (Dez. 17, 2007). *Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de Dezembro de 2007*. (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12007L%2FTXT

Assembleia da República. (Ago. 24, 2007). *Lei n.º 46/2007, de 24 de agosto*. (Consultado em jan. 12, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/46-2007-640919

Roque, A., Lobo, C., Andrade L., António H., Barroso, L., Almeida, V., & Silveira, L. (Set. 13, 2010). *Deliberação n.º 629/2010: Princípios aplicáveis ao tratamento de dados de gravação de chamadas*. (Consultado em jan. 12, 2025). Obtido de Comissão Nacional de Proteção de Dados (CNPD): https://www.cnpd.pt/media/q01alptr/del629_2010.pdf

União Europeia. (Mar. 9, 2011). *Directiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de Março de 2011 , relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços*. (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32011L0024

Nações Unidas. (Jan. 21, 2014). *Resolution adopted by the General Assembly on 18 December 2013*. (Consultado em jan. 12, 2025). Obtido de Nações Unidas: https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf

União Europeia. (Jul. 25, 2014). *Regulamento Delegado (UE) n. ° 1042/2014 da Comissão, de 25 de julho de 2014 , que completa o Regulamento (UE) n. ° 514/2014 no que se refere à designação e às competências de gestão e de controlo das autoridades responsáveis, e no que se refere ao estatuto e obrigações das autoridades de auditoria*. (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32014R1042

União Europeia. (Abr. 27, 2016). *Regulamento (UE) 2016/679 do Parlamento Europeu 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 e que revoga a Diretiva 95/46/CE* (Consultado em jan. 12, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679

Gabinete do Secretário de Estado da Saúde. (Fev. 8, 2017). *Despacho n.º 1348/2017, de 8 de fevereiro.* (Consultado em jan. 13, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/despacho/1348-2017-106415139

Assembleia da República. (Ago. 8, 2019). *Lei n.º 58/2019, de 8 de agosto*. (Consultado em jan. 13, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Assembleia da República. (Abr. 27, 2019). *Lei n.º 59/2019, de 8 de agosto*. (Consultado em jan. 13, 2025). Obtido de Diário da República: https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983

União Europeia. (Maio 3, 2022). *Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao Espaço Europeu de Dados de Saúde*. (Consultado em jan. 13, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52022PC0197

União Europeia. (Dez. 14, 2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o*

910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148). (Consultado em jan. 13, 2025). Obtido de União Europeia: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555

Conselho da União Europeia. (Jan. 21, 2025). *Espaço Europeu de Dados de Saúde: Conselho adota novo regulamento que melhora o acesso transfronteiriço aos dados de saúde na EU*. (Consultado em fev. 14, 2025). Obtido de Conselho da UE: https://www.consilium.europa.eu/pt/press/press-releases/2025/01/21/european-health-data-space-council-adopts-new-regulation-improving-cross-border-access-to-eu-health-data/

Comissão Europeia. (Dez. 16, 2020). *Comission Staff Working Document: Impact Assessment Report*. (Consultado em fev. 17, 2025). Obtido de CE: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020SC0345

Ministério dos Negócios Estrangeiros. (Jul. 31, 2014). *Manual de Boas Práticas para a Negociação, Transposição e Aplicação de Legislação da União Europeia*. (Consultado em fev. 26, 2025). Obtido de Direção Geral da Política de Justiça: https://dgpj.justica.gov.pt/Portals/31/AIN_Programas/Transposi%E7%E3o_atempada_MNE.pdf

Hollweck, T. (2015). Robert K. Yin.(2014). *Case Study Research Design and Methods*. (Consultado em mar. 11, 2025). Obtido de Canadian Journal of Program Evaluation, 30(1), 108-110: https://utppublishing.com/doi/pdf/10.3138/cjpe.30.1.108

Grand Canyon University. (Oct. 9, 2023). Qualitative vs. Quantitative Research: What's the Difference? (Consultado em mar. 14, 2025). Obtido de Grand Canyon University: https://www.gcu.edu/blog/doctoral-journey/qualitative-vsquantitative-research-whats-difference

Apêndices

Apêndice A – Questionário sobre tratamento e proteção de dados na emergência pré-hospitalar

Tratamento e proteção de dados na emergência pré-hospitalar

Caro/a participante,

O presente questionário online, elaborado por Tiago Monteiro e orientado pelo Prof. Rui Rijo, enquadra-se no âmbito da Unidade Curricular Projeto, do 2º ano do Mestrado em Cibersegurança e Informática Forense, ministrado pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Como principais objetivos deste estudo, pretende-se avaliar os procedimentos de tratamento e proteção de dados adotados pelas equipas de emergência, identificar desafios práticos no cumprimento das normas legais e, ainda, compreender o impacto e as implicações éticas que a legislação acarreta para as operações de socorro.

A sua participação é voluntária e anónima. No uso que se realize dos resultados do estudo, com fins de ensino, investigação e/ou publicação, respeitar-se-á sempre a devida anonimização dos dados obtidos, de modo que cada participante não será identificado ou identificável. Poderá desistir de participar em qualquer momento do questionário ou retirar a autorização para utilizar os seus dados, de acordo com a Lei nº 58/2019.

O questionário estará disponível até 20 de abril de 2025 e o seu preenchimento demorará cerca de 10 minutos.

Em caso de dúvidas pode contactar o autor responsável através do e-mail 2230466@my.ipleiria.pt.

Secção 1

Consentimento informado, livre e esclarecido

1. Declara que tomou conhecimento da informação acima e que está de acordo em participar voluntariamente neste estudo?

- o Sim
- o Não

Secção 2

Caracterização sociodemográfica

2. Género:

- Masculino
- Feminino
- Não quero indicar / Outro

3. Faixa etária:

- Menos de 20 anos
- 21 a 30 ano
- 31 a 40 anos
- 41 a 50 anos
- Mais de 50 anos

4. Escolaridade:

- Inferior ao 9º ano
- 9º ano ou equivalente
- 12º ano ou equivalente
- CET/CTeSP
- Licenciatura
- Mestrado
- Doutoramento

5. Região:

- Norte
- Centro
- Lisboa e Vale do Tejo
- Alentejo
- Algarve
- Açores/Madeira

6. Tempo de serviço:

- Menos de 5 anos
- 6 a 10 anos
- 11 a 15 anos

- 16 a 20 anos
- Mais de 25 anos

7. Vínculo institucional:

- Profissional
- Voluntário

8. Função desempenhada:

- TAT
- TAS
- TEPH
- Enfermeiro
- Médico
- Outro

Secção 3

Perceção sobre a legislação vigente

9. Conhece a regulamentação europeia e a legislação nacional sobre proteção de dados pessoais e sensíveis?

- Sim
- Não
- Parcialmente

10. Já teve formação específica sobre proteção de dados pessoais e/ou sensíveis?

- Sim, há mais de 5 anos
- Sim, há menos de 5 anos
- Não
- Não, mas gostaria de ter

11. Onde foi obtida a formação?

- A nível pessoal
- Dentro da minha instituição
- Através de entidade externa

12. Sabe distinguir dados pessoais de dados "sensíveis" nos termos da lei?

- Sim

- Não
- Não tenho a certeza

13. Acha que é necessário obter o consentimento da vítima antes de recolher os seus dados pessoais?

- Sim, sempre
- Nem sempre
- Não, nunca

14. Tem conhecimento do princípio da "minimização dos dados"?

- Sim, sei o que significa
- Já ouvi falar, mas não sei exatamente o que é
- Não, nunca ouvi falar

Secção 4

Avaliação de conhecimentos práticos

15. **Cenário:** Durante o preenchimento do verbete de emergência médica, recolhe diversas informações sobre a vítima.
Pergunta: Quais dos seguintes dados são considerados, segundo a legislação, "categorias especiais de dados" (dados sensíveis)?

- Grupo sanguíneo, contactos de emergência e medicação habitual.
- Nome completo, morada e número de telefone.
- Religião, dados relativos à saúde e orientação sexual.
- Dados genéticos, sinais vitais e nome completo.

16. **Cenário:** Chega a um acidente rodoviário e precisa de recolher dados de saúde de uma vítima consciente para preencher o verbete de emergência médica.
Pergunta: O que deve fazer antes de recolher esses dados?

- Informar a vítima, obtendo o seu consentimento, salvo se isso atrasar significativamente o socorro.
- Informar a vítima e obter o seu consentimento, exceto se a recolha de dados resultar de uma obrigação legal ou de interesse vital.
- Apenas recolher dados pessoais após contactar o CODU e obter instruções específicas.

- Recolher os dados imediatamente, pois a recolha de informação é prioritária face à necessidade de consentimento.

17. **Cenário:** Durante a assistência a uma vítima inconsciente, um indivíduo chega ao local, informa ser familiar e solicita informações detalhadas sobre o estado de saúde da vítima.
Pergunta: Como deve agir neste caso?

- Transmitir o estado clínico completo, pois há um interesse legítimo da família em ser informada.
- Comunicar informações básicas (ex. estado de consciência), respeitando a confidencialidade e avaliando caso a caso.
- Não divulgar qualquer informação, salvo autorização expressa da vítima ou obrigação legal.
- Partilhar as informações estritamente necessárias, desde que o familiar prove a sua ligação e o conhecimento seja indispensável.

18. **Cenário:** Necessita de passar dados sobre a situação de uma vítima ao CODU. Tem disponível o rádio portátil e o telemóvel de serviço/pessoal.
Pergunta: Qual o meio mais adequado para garantir a proteção dos dados pessoais?

- O telefone, pois a transmissão é mais segura e permite maior confidencialidade.
- O canal mais rápido e disponível, assegurando que a informação não inclui identificação direta da vítima.
- Ambos os meios são adequados, se seguir os protocolos institucionais de comunicação.
- O rádio, se for mais rápido, desde que use apenas informações clínicas indispensáveis.

19. **Cenário:** Após a ocorrência, tem anotações com dados da vítima que usou para preencher o verbete.
Pergunta: O que deve fazer com esses apontamentos?

- Remeter os apontamentos a um superior hierárquico para decisão sobre a conservação.
- Guardar os dados durante 30 dias para eventual consulta em caso de auditoria ou reclamação da vítima.

- Destruir ou eliminar imediatamente as anotações após cumprida a finalidade para que foram recolhidas.
- Arquivar os dados num local seguro, em conformidade com a política de conservação de dados da entidade.

20. **Cenário:** Durante a recolha de dados pessoais e clínicos de uma vítima consciente, esta questiona por que motivo estão a ser recolhidas essas informações e como serão tratadas.
Pergunta: Que informações deve obrigatoriamente prestar à vítima?

- Apenas que os dados são recolhidos no âmbito da emergência, sem necessidade de explicar detalhes adicionais.
- Informar que os dados são tratados para a prestação de cuidados de saúde e que tem o direito de saber as finalidades do tratamento, os destinatários, o prazo de conservação e outros aspetos previstos na lei.
- Explicar que os dados são recolhidos por rotina operacional e que qualquer dúvida deve ser colocada à CNPD.
- Dizer que, por ser um ambiente de emergência, não existe obrigatoriedade de prestar esclarecimentos adicionais.

21. **Cenário:** Após uma ocorrência, recebe uma notificação da Comissão Nacional de Proteção de Dados (CNPD), solicitando prova de que obteve o consentimento da vítima para o tratamento dos dados pessoais recolhidos durante o socorro.
Pergunta: Como deve demonstrar que cumpriu essa obrigação?

- Enviar o verbete de emergência ou o registo onde consta a anotação de que o consentimento foi solicitado e obtido, de acordo com o procedimento habitual.
- Declarar que, em contexto de emergência, o consentimento pode ser implícito, não sendo necessária documentação adicional.
- Explicar que o consentimento foi obtido verbalmente, mas que não existe registo formal que o demonstre porque a prioridade foi assegurar o socorro imediato.
- Remeter a documentação da ocorrência para a entidade hospitalar, solicitando que esta responda diretamente à CNPD com os dados disponíveis.

22. **Cenário:** Durante o atendimento, a vítima fornece os seus dados pessoais e autoriza o seu tratamento. No final da ocorrência, a vítima pergunta se pode retirar o consentimento dado para o tratamento dos seus dados.
Pergunta: O que deve esclarecer?

- Informar que, por se tratar de um serviço de emergência, não é possível retirar o consentimento após o seu fornecimento.
- Afirmar que a retirada do consentimento só pode ser feita junto da autoridade de controlo (CNPD).
- Explicar que a vítima tem o direito de retirar o consentimento a qualquer momento.
- Dizer que, como o consentimento foi dado verbalmente, não é reconhecido o direito de o retirar.

23. **Cenário:** Durante a assistência a vítimas num acidente, um jornalista aproxima-se e solicita informações sobre a identidade e estado de saúde das pessoas assistidas.
Pergunta: Como deve agir?

- Fornecer informações básicas, como idade, género e estado de consciência, pois o interesse público justifica a divulgação.
- Recusar prestar qualquer informação pessoal ou clínica, invocando o dever de confidencialidade e proteção de dados.
- Partilhar os dados, desde que o jornalista garanta que serão utilizados de forma ética e respeitosa.
- Indicar apenas a quantidade de vítimas e o tipo de ocorrência, sem divulgar qualquer dado pessoal ou de saúde.

24. **Cenário:** Após prestar socorro a uma vítima, um agente de autoridade pede-lhe informações detalhadas sobre o estado de saúde e dados pessoais dessa pessoa, alegando necessidade para o auto de ocorrência.
Pergunta: Como deve proceder?

- Fornecer os dados pessoais e clínicos necessários para a realização do auto de ocorrência.
- Facultar todos os dados pessoais e clínicos completos, sem qualquer restrição, uma vez que a PSP tem sempre direito a esta informação.
- Encaminhar o pedido para o CODU ou para a unidade hospitalar, por serem as únicas entidades autorizadas a fornecer informações à autoridade policial.
- Recusar a prestação de qualquer informação sem ordem judicial ou consentimento prévio da vítima.

Secção 5

Desafios e melhorias

25. Quais são, na sua opinião, os principais desafios na aplicação da legislação sobre proteção de dados no contexto pré-hospitalar? (Selecione todas as opções que se aplicam)

- □ Complexidade e dispersão do enquadramento legal aplicável à proteção de dados de saúde.
- □ Falta de formação específica dos profissionais de emergência sobre proteção de dados.
- □ Ausência de procedimentos uniformes para registo do consentimento.
- □ Dificuldade em garantir a confidencialidade em locais públicos.
- □ Conflito de princípios com a necessidade de partilhar informações com hospitais, forças de segurança, etc.
- □ Falta de mecanismos/recursos de gestão e conservação da informação pós-evento.
- □ Outros

26. Se selecionou "Outros" na pergunta anterior, descreva outros desafios que enfrenta.

(Introduza a sua resposta)

27. Quais são, na sua opinião, as principais melhorias necessárias para o aumento geral do nível de proteção de dados no contexto pré-hospitalar? (Selecione todas as opções que se aplicam)

- □ Criação de um guia prático ou manual simplificado, que reúna as principais normas de proteção de dados aplicáveis à emergência pré-hospitalar.
- □ Formação contínua e obrigatória em proteção de dados para profissionais de emergência.
- □ Definição de protocolos claros para a recolha e registo do consentimento como, por exemplo, um campo específico nos verbetes de emergência médica.
- □ Designação de Encarregados de Proteção de Dados (EPD) nas corporações, com responsabilidade de supervisão e apoio às equipas no terreno.
- □ Disponibilização de dispositivos de comunicação seguros como telemóveis exclusivos ao serviço.
- □ Criação de auditorias e inspeções regulares para monitorização do cumprimento das normas de proteção de dados.
- □ Outros

28. Se selecionou "Outros" na pergunta anterior, descreva outras melhorias que sugere.

(Introduza a sua resposta)

Apêndice B – Email de divulgação do questionário

Exmos. Senhores,

Espero que se encontrem bem.

O meu nome é Tiago Monteiro, sou Bombeiro Voluntário em Viseu e aluno do curso de Mestrado em Cibersegurança e Informática Forense, no Instituto Politécnico de Leiria. No âmbito da minha dissertação, intitulada "Tratamento e Proteção de Dados na Emergência Pré-Hospitalar", desenvolvi um estudo que visa avaliar o conhecimento, as práticas e os desafios que os profissionais de emergência enfrentam no tratamento de dados pessoais e de saúde das vítimas.

Para tal, elaborei um questionário anónimo e de preenchimento voluntário, dirigido exclusivamente a profissionais de emergência pré-hospitalar, como técnicos de emergência pré-hospitalar, tripulantes de ambulância de socorro e de transporte, médicos e enfermeiros, entre outros.

Neste sentido, venho por este meio solicitar a vossa colaboração para a divulgação deste questionário junto de todo o vosso efetivo, através dos canais de comunicação internos que considerem mais adequados (e-mail, redes sociais, grupos de mensagens, etc.).

O tempo estimado de resposta é inferior a 10 minutos e não são recolhidos quaisquer dados pessoais ou identificadores, respeitando integralmente as normas de ética e proteção de dados em vigor. O período de recolha de respostas termina no próximo dia 20/04.

O link de acesso ao questionário é o seguinte:

👉 https://forms.office.com/e/kJZGL8xch8

Agradeço, desde já, a vossa atenção e disponibilidade para colaborar com este projeto, que pretende contribuir para uma maior consciencialização e boas práticas no manuseamento de dados pessoais em contexto de emergência pré-hospitalar.

Para qualquer esclarecimento adicional, estarei totalmente disponível através do endereço de email 2230466@my.ipleiria.pt.

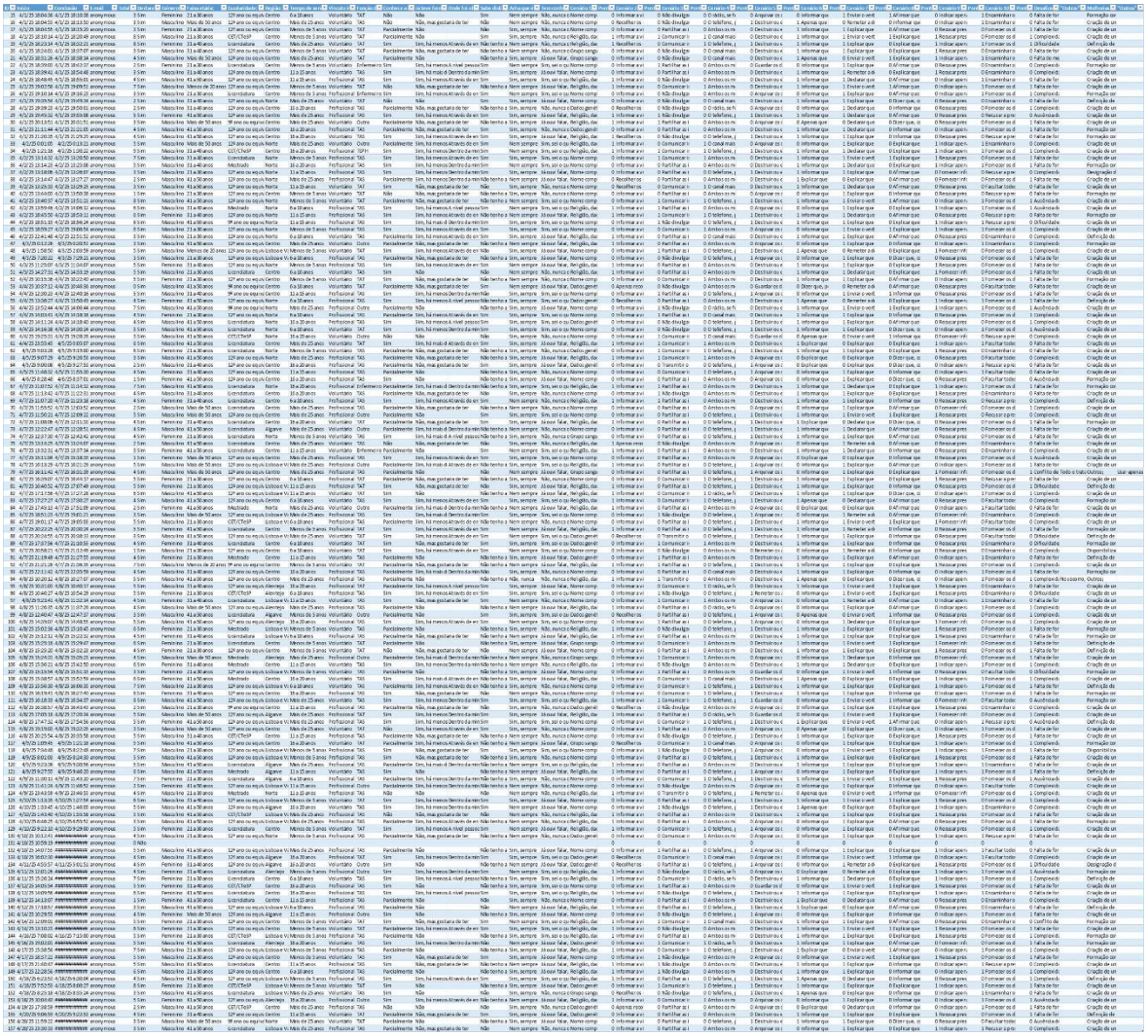
Com os melhores cumprimentos,

Tiago Monteiro

Apêndice C – Transcrição integral das respostas recolhidas dos revisores

ID	1	2	3	4
Hora de inicio	2025-03-23 13:06:34	2025-03-23 14:16:21	2025-03-23 14:34:49	2025-03-23 15:31:33
Hora de conclusão	2025-03-23 13:25:39	2025-03-23 14:24:48	2025-03-23 14:40:39	2025-03-23 15:53:16
E-mail	anonymous	anonymous	anonymous	anonymous
Declara que tomou conhecimento da informação acima e que está de acordo em participar voluntariamente neste estudo?	Sim	Sim	Sim	Sim
Género:	Masculino	Masculino	Feminino	Masculino
Faixa etária:	Mais de 50 anos	21 a 30 anos	31 a 40 anos	31 a 40 anos
Escolaridade:	Mestrado	Licenciatura	Licenciatura	12º ano ou equivalente
Região:	Centro	Centro	Centro	Centro
Tempo de serviço:	Mais de 25 anos	Menos de 5 anos	11 a 15 anos	16 a 20 anos
Vínculo institucional:	Profissional	Voluntário	Voluntário	Profissional
Função desempenhada:	Enfermeiro	TAT	TAT	TAS
Conhece a regulamentação europeia e a legislação nacional sobre proteção de dados pessoais e sensíveis?	Parcialmente	Não	Parcialmente	Parcialmente
Já teve formação específica sobre proteção de dados pessoais e/ou sensíveis?	Sim, há menos de 5 anos	Não, mas gostaria de ter	Não, mas gostaria de ter	Sim, há menos de 5 anos
Onde foi obtida a formação?	Dentro da minha instituição			Dentro da minha instituição
Sabe distinguir dados pessoais de dados "sensíveis" nos termos da lei?	Não	Não tenho a certeza	Não tenho a certeza	Não tenho a certeza
Acha que é necessário obter o consentimento da vítima antes de recolher os seus dados pessoais?	Sim, sempre	Nem sempre	Nem sempre	Nem sempre
Tem conhecimento do princípio da "minimização dos dados"?	Não, nunca ouvi falar	Já ouvi falar, mas não sei exatamente o que é	Não, nunca ouvi falar	Já ouvi falar, mas não sei exatamente o que é
Cenário 1	Grupo sanguíneo, contactos de emergência e medicação habitual.	Grupo sanguíneo, contactos de emergência e medicação habitual.	Grupo sanguíneo, contactos de emergência e medicação habitual.	Nome completo, morada e número de telefone.
Cenário 2	Informar a vítima, obtendo o seu consentimento, salvo se isso atrasar significativamente o socorro.	Informar a vítima e obter o seu consentimento, exceto se a recolha de dados resultar de uma obrigação legal ou de interesse vital.	Informar a vítima e obter o seu consentimento, exceto se a recolha de dados resultar de uma obrigação legal ou de interesse vital.	Informar a vítima e obter o seu consentimento, exceto se a recolha de dados resultar de uma obrigação legal ou de interesse vital.
Cenário 3	Não divulgar qualquer informação clínica, salvo autorização expressa da vítima ou obrigação legal.	Comunicar informações básicas (ex. estado de consciência), respeitando a confidencialidade e avaliando caso a caso.	Não divulgar qualquer informação, salvo autorização expressa da vítima ou obrigação legal.	Não divulgar qualquer informação, salvo autorização expressa da vítima ou obrigação legal.
Cenário 4	O telefone, pois a transmissão é mais segura e permite maior confidencialidade.	Ambos os meios são adequados, se seguir os protocolos institucionais de comunicação.	Ambos os meios são adequados, se seguir os protocolos institucionais de comunicação.	O telefone, pois a transmissão é mais segura e permite maior confidencialidade.
Cenário 5	Arquivar os dados num local seguro, em conformidade com a política de conservação de dados da entidade.	Arquivar os dados num local seguro, em conformidade com a política de conservação de dados da entidade.	Destruir ou eliminar imediatamente as anotações após cumprida a finalidade para que foram recolhidas.	Destruir ou eliminar imediatamente as anotações após cumprida a finalidade para que foram recolhidas.
Cenário 6	Informar que os dados são tratados para a prestação de cuidados de saúde e que tem o direito de saber as finalidades do tratamento, os destinatários, o prazo de conservação e outros aspetos previstos na lei.	Informar que os dados são tratados para a prestação de cuidados de saúde e que tem o direito de saber as finalidades do tratamento, os destinatários, o prazo de conservação e outros aspetos previstos na lei.	Informar que os dados são tratados para a prestação de cuidados de saúde e que tem o direito de saber as finalidades do tratamento, os destinatários, o prazo de conservação e outros aspetos previstos na lei.	Informar que os dados são tratados para a prestação de cuidados de saúde e que tem o direito de saber as finalidades do tratamento, os destinatários, o prazo de conservação e outros aspetos previstos na lei.
Cenário 7	Explicar que o consentimento foi obtido verbalmente, mas que não existe registo formal porque a prioridade foi assegurar o socorro imediato.	Explicar que o consentimento foi obtido verbalmente, mas que não existe registo formal porque a prioridade foi assegurar o socorro imediato.	Declarar que, em contexto de emergência, o consentimento pode ser implícito, não sendo necessária documentação adicional.	Explicar que o consentimento foi obtido verbalmente, mas que não existe registo formal porque a prioridade foi assegurar o socorro imediato.
Cenário 8	Explicar que a vítima tem o direito de retirar o consentimento a qualquer momento, sem prejuízo para a licitude do tratamento efetuado até esse momento.	Explicar que a vítima tem o direito de retirar o consentimento a qualquer momento, sem prejuízo para a licitude do tratamento efetuado até esse momento.	Explicar que a vítima tem o direito de retirar o consentimento a qualquer momento, sem prejuízo para a licitude do tratamento efetuado até esse momento.	Explicar que a vítima tem o direito de retirar o consentimento a qualquer momento, sem prejuízo para a licitude do tratamento efetuado até esse momento.
Cenário 9	Indicar apenas a quantidade de vítimas e o tipo de ocorrência, sem divulgar qualquer dado pessoal ou de saúde.	Indicar apenas a quantidade de vítimas e o tipo de ocorrência, sem divulgar qualquer dado pessoal ou de saúde.	Recusar prestar qualquer informação pessoal ou clínica, invocando o dever de confidencialidade e proteção de dados.	Indicar apenas a quantidade de vítimas e o tipo de ocorrência, sem divulgar qualquer dado pessoal ou de saúde.
Cenário 10	Encaminhar o pedido para o CODU ou para a unidade hospitalar, por serem as únicas entidades autorizadas a fornecer informações à autoridade policial.	Fornecer os dados pessoais e clínicos necessários para a realização do auto de ocorrência.	Fornecer os dados pessoais e clínicos necessários para a realização do auto de ocorrência.	Fornecer os dados pessoais e clínicos necessários para a realização do auto de ocorrência.
Desafios?	Falta de formação específica dos profissionais de emergência sobre proteção de dados.;Ausência de procedimentos uniformes para registo do consentimento.;Dificuldade em garantir a confidencialidade em locais públicos.;	Complexidade e dispersão do enquadramento legal aplicável à proteção de dados de saúde.;Falta de formação específica dos profissionais de emergência sobre proteção de dados.;Dificuldade em garantir a confidencialidade em locais públicos.;	Falta de formação específica dos profissionais de emergência sobre proteção de dados.;Ausência de procedimentos uniformes para registo do consentimento.;Complexidade e dispersão do enquadramento legal aplicável à proteção de dados de saúde.;Conflito de princípios com a necessidade de partilhar informações com hospitais, forças de segurança, etc.;	Falta de formação específica dos profissionais de emergência sobre proteção de dados.;Dificuldade em garantir a confidencialidade em locais públicos.;Conflito de princípios com a necessidade de partilhar informações com hospitais, forças de segurança, etc.;Falta de mecanismos/recursos de gestão da informação pós-evento.;
Melhorias?	Criação de um guia prático ou manual simplificado, que reúna as principais normas de proteção de dados aplicáveis à emergência pré-hospitalar.;Formação contínua e obrigatória em proteção de dados para profissionais de emergência.;Definição de protocolos claros para a recolha e registo do consentimento como, por exemplo, um campo específico nos verbetes de emergência médica.;	Formação contínua e obrigatória em proteção de dados para profissionais de emergência.;Definição de protocolos claros para a recolha e registo do consentimento como, por exemplo, um campo específico nos verbetes de emergência médica.;Criação de auditorias e inspeções regulares para monitorização do cumprimento das normas de proteção de dados.;	Formação contínua e obrigatória em proteção de dados para profissionais de emergência.;Definição de protocolos claros para a recolha e registo do consentimento como, por exemplo, um campo específico nos verbetes de emergência médica.;Designação de Encarregados de Proteção de Dados (EPD) nas corporações, com responsabilidade de supervisão e apoio às equipas no terreno.;Disponibilização de dispositivos de comunicação seguros como telemóveis exclusivos ao serviço.;Criação de um guia prático ou manual simplificado, que reúna as principais normas de proteção de dados aplicáveis à emergência pré-hospitalar.;Criação de auditorias e inspeções regulares para monitorização do cumprimento das normas de proteção de dados.;	Formação contínua e obrigatória em proteção de dados para profissionais de emergência.;Definição de protocolos claros para a recolha e registo do consentimento como, por exemplo, um campo específico nos verbetes de emergência médica.;Designação de Encarregados de Proteção de Dados (EPD) nas corporações, com responsabilidade de supervisão e apoio às equipas no terreno.;Criação de auditorias e inspeções regulares para monitorização do cumprimento das normas de proteção de dados.;

Apêndice D – Transcrição integral das respostas recolhidas de todos os participantes



Apêndice E – Exemplo de guia rápido e prático para consulta dos profissionais

1. Princípios Fundamentais

Confidencialidade: Todos os dados recolhidos no local da ocorrência são confidenciais.

Minimização: Apenas devem ser recolhidos os dados estritamente necessários.

Finalidade: Os dados só podem ser usados para a prestação de cuidados e comunicação com entidades envolvidas no socorro.

Segurança: Garantir proteção física e digital dos dados recolhidos.

2. Consentimento da Vítima

Sempre que possível, solicitar o consentimento verbal da vítima antes de recolher e transmitir dados de saúde.

Registar no campo de observações do verbete que o consentimento foi obtido verbalmente.

Se a vítima estiver inconsciente ou incapacitada, agir com base no interesse vital, minimizando os dados partilhados.

Se a vítima não consentir com a recolha dos dados, a mesma não deve ser feita.

Pedidos de reclamação, retificação, apagamento, portabilidade de dados, entre outros direitos, devem ser realizados diretamente à entidade responsável (INEM).

3. Partilha de Informação

Só deve ocorrer com entidades que participam diretamente no socorro (hospital, INEM, forças de segurança, etc).

Em locais públicos, privilegiar a partilha de dados dentro da célula da ambulância ou em ambientes resguardados.

Evitar discutir dados clínicos em voz alta junto de terceiros.

4. Equipamentos e Documentação

Conservar verbetes em locais trancados e acessíveis apenas a pessoal autorizado.

Utilizar exclusivamente, e se possível, os equipamentos fornecidos pela entidade, evitando comunicações por dispositivos pessoais.

Manter o iTeams desligado de redes públicas e armazenado em local seguro fora da utilização.

5. Responsabilidade e Sigilo

Recordar que todos os profissionais estão legalmente vinculados ao dever de sigilo.

A partilha indevida de dados pode acarretar responsabilidade disciplinar e criminal.

6. Apoio Institucional

Procurar esclarecimento junto do Encarregado de Proteção de Dados (DPO) do responsável pelo tratamento (INEM) em caso de dúvida.

Participar em ações de formação sobre proteção de dados sempre que disponibilizadas.

Nota: Este guia é um apoio operacional e não substitui a leitura integral dos normativos legais em vigor. Para uma abordagem mais detalhada, consultar o trabalho "Tratamento e Proteção de Dados na Emergência Pré-Hospitalar", de Tiago Monteiro.

Apêndice F – Artigo desenvolvido e submetido para publicação

(Apresentado na íntegra a partir da página seguinte)

Data Processing and Protection in Pre-Hospital Emergency Care

Tiago Monteiro*, Rui Rijo*†
*School of Technology and Management, Polytechnic Institute of Leiria, Leiria, Portugal
Email: 2230466@my.ipleiria.pt
†Institute for Systems Engineering and Computers at Coimbra, Coimbra, Portugal
Email: rui.rijo@ipleiria.pt

***Abstract*—Every day, prehospital emergency professionals handle personal and health-related data, the protection of which is crucial to safeguard victims' privacy, prevent unauthorized access, and ensure legal compliance. This article examines the rights and duties of both victims and responders—before, during, and after the provision of care—through the analysis and synthesis of the extensive and specific European and Portuguese legal framework. In addition, it presents a practical case study that assesses the level of awareness among a sample of professionals regarding data protection and proposes some policy-making actions to improve the present scenario. The study therefore addresses the relevant literature, the types of services and data involved in an emergency event, the applicable legislation and regulations, the challenges faced by professionals in the field, the legal rights of data subjects, the methodology applied in the case study, the results obtained, and, finally, the main conclusions.**

***Index Terms*—Prehospital emergency care, Health data, Privacy, Legislation, Awareness**

I. Introduction

The increasing digitalization of healthcare services has brought new challenges regarding the protection of patient privacy, especially in contexts where urgency and operational mobility hinder the strict application of legal principles. Prehospital emergency care, as the first line of response, represents one of these critical contexts, where the collection, processing, and transmission of sensitive data often take place under unstable, unpredictable, and exposed conditions.

Despite the various advances achieved over recent decades in establishing a robust regulatory framework for data processing, practical weaknesses persist in the application and enforcement of these rules—particularly among professionals who, although although well-intentioned, often act based on outdated or inaccurate perceptions of their legal responsibilities. The dispersion of legislation, the technical and legal terminology, and the complexity of the prehospital emergency environment—characterized by multiple actors and diverse operational scenarios—further intensify these challenges, making a specific and in-depth analysis of this field essential.

In this context, the present article focuses on the Portuguese reality and aims to synthesize the applicable legal framework, understand the challenges faced by emergency teams, explore their perceptions of the legal responsibilities imposed, and contribute to the identification of strategies that can enhance data security for victims without compromising the quality or readiness of emergency care.

II. Literature Review

The literature review provides a comprehensive overview of the existing approaches and practices regarding data protection in emergency contexts, aims to identify the contributions, limitations, and trends of these works, in order to frame the relevance and objectives of the present study.

A. Methodology

The establishment of clear and concrete criteria for the literature search is essential to ensure that any review is both relevant and robust.

Accordingly, the research was initially based on the axes of concept, context, and perspective [1]: data protection in prehospital emergencies, the specific emergency situations in which data processing occurs, and the analysis of data protection practices.

Subsequently, sources were selected through searches conducted on platforms such as Google Scholar, Scopus, b-on, EBSCO, JSTOR, ResearchGate, and IEEE Explore, using filters by publication date (less than 10 years), thematic area, and relevance. Additionally, institutional manuals (e.g. TAS INEM manual), and official sources (INEM website) were explored. Some of the keywords used included "prehospital emergency care", "data protection emergency care", "data privacy healthcare", "GDPR emergency care", "prehospital care", "digital privacy in healthcare", "patient data protection", and other related combinations.

After selecting credible scientific publications closely aligned with the purpose of this study, the research was considered complete upon reaching theoretical saturation. Of the approximately 20 related works identified, only 14 were analyzed in this paper. This structured approach ensured a comprehensive review, aligned with the objectives of the study.

B. Related Work

Based on the aforementioned criteria, several articles and reports were selected for the analysis of their key findings.

In 2022, Carina Carvalho [2] examined the application of the GDPR in primary healthcare in Portugal, highlighting operational and ethical challenges in managing sensitive data. The author concluded that despite increased institutional awareness, implementation has been hindered by limited professional training and the complexity of the legal framework,

particularly within the public sector, which often lacks sufficient resources.

Gonçalo Nunes [3] explored the evolution of fundamental rights in the context of personal health data protection, emphasizing the impact of the GDPR in enhancing privacy and strengthening data subjects' rights. He highlighted the relevance of principles such as privacy by design and privacy by default, and the need to balance information protection with public interests like scientific research, calling for a careful integration of ethics, security, and innovation in healthcare.

Similarly, Ana Rio Tinto [4] analyzed health data protection within hospital settings, focusing on hospital administrators' knowledge of GDPR requirements. Through questionnaires, the study revealed significant weaknesses in professionals' preparedness, particularly regarding data subject rights and security measures. The findings reinforced the need for structured training and strategic integration of data protection within healthcare institutions.

Beyond academia, public and governmental organizations have also published guidelines to support legal compliance and dissemination. One such example is the guide published by the Shared Services of the Ministry of Health (SPMS) [5] on information privacy in the healthcare sector. The document addresses the challenges of digital transformation and the need to adapt to the GDPR, detailing legal obligations, security measures, and good practices tailored to different professional roles. It emphasizes the importance of continuous training, impact assessments, and the appointment of a Data Protection Officer (DPO) as essential pillars to ensure data protection and trust within integrated care ecosystems.

The Portuguese National Institute of Medical Emergency (INEM) Ambulance Crew Manual [6] includes a section dedicated to data protection, outlining the legal grounds for collecting and processing personal and health data. It clarifies consent principles, including exceptions for incapacitated individuals, and reinforces that processing is only lawful when performed by professionals bound by confidentiality obligations. It also outlines data subject rights, such as access, rectification, and erasure, aligning operational practices with GDPR requirements.

Another study [7] conducted a literature review on digital privacy in prehospital emergency contexts, concluding that the topic remains underexplored. It identified factors such as responder training and operational conditions as key to data protection, and called for greater awareness and scientific investigation in this specific scenario.

A conference paper [8] reviewed data protection strategies in the healthcare sector, emphasizing the urgency of strengthening safeguards in response to growing digitalization and associated threats. Using bibliometric analysis, the authors highlighted the importance of data governance, legal compliance, and the adoption of international standards as fundamental pillars for securing information in healthcare organizations.

In a Nordic context, several authors proposed the HSPAMI model to align healthcare professionals' security practices with international regulations [9]. The study identified discrepancies between actual behaviors and legal requirements, emphasizing that healthcare professionals remain a critical weak link. It also reinforced the importance of training and awareness as key strategies for fostering a strong information security culture.

Addressing the challenges of cybersecurity, two studies [10], [11] focused on the increasing digital vulnerabilities in healthcare. They emphasized the need for a robust security culture, ongoing training, and the adoption of international frameworks like NIST and ISO. The use of emerging technologies such as AI and blockchain was recommended, along with collaborative efforts between public entities and professionals to enhance system resilience and user trust.

Emergency medicine and prehospital care share similar challenges concerning privacy and confidentiality. In this regard, two earlier articles [12], [13], though published in 2005 and 2006, remain relevant by addressing the ethical and legal obligations tied to patient information protection in emergency settings. The authors clearly distinguish between privacy and confidentiality and explore practical challenges such as emergency room design and third-party presence. They argue that, even in high-pressure environments, safeguarding patient information must prevail, with exceptions being rare and justified.

In Turkey, Hasan Erbay discussed ethical dilemmas in prehospital care [14], highlighting the difficulty of ensuring privacy and confidentiality in unstable and public environments. The study noted that emergency responders often face conflicts between rapid care delivery and respecting victims' dignity, underscoring the need for solid training and tailored protocols to guide responsible decision-making in unpredictable situations.

Finally, in 2019, researchers in Finland [15] investigated paramedics' perceptions of informational privacy in prehospital care, identifying factors that influence its protection. While acknowledging the importance of confidentiality, the study revealed practical variability, shaped by training, work environment, and professional attitudes. The authors emphasized the need to strengthen training and provide clear guidelines to ensure effective protection of sensitive data in emergency contexts.

In summary, the reviewed literature shows that data protection in the healthcare sector has been widely explored in recent years. However, a significant gap remains regarding the prehospital emergency context, which is still largely overlooked. Most studies focus on hospital environments and the challenges of implementing the GDPR, with few addressing the unique limitations of prehospital care.

Nevertheless, the studies converge on several key points: the importance of the GDPR as a legal milestone; the need to uphold confidentiality and professional secrecy; the practical difficulties in adapting to the regulations; the urgency for structured governance; and, above all, the fragility of professional training in this area.

III. Pre-Hospital Emergency

To frame data protection legislation within the context of pre-hospital emergency care, it is essential first to understand the definition and general functioning of this area, as well as to be familiar with the emergency services operating in Portugal.

Medical emergency refers to any sudden and unexpected situation that poses an immediate risk to a person's life or health, requiring rapid medical intervention to prevent deterioration or death [16]. Pre-hospital emergency, in turn, concerns the assistance to victims who experience episodes requiring urgent or emergency care before reaching the hospital [17].

In Portugal, an average of 4,149 medical emergency calls per day were recorded in 2023 [18], illustrating the high frequency and complexity of such incidents. The response is ensured by various entities, such as the National Institute of Medical Emergency (INEM), the Fire Departments, and the Portuguese Red Cross. This multiplicity of actors, combined with the daily volume of occurrences, results in a vast amount of personal and clinical data being shared constantly among different professionals and institutions.

In an emergency situation, information typically collected includes the name, age, sex, contact details, National Health Service (SNS) user number, vital signs, clinical condition, usual medication, relevant medical history, and circumstances of the incident. Currently, this data is initially recorded by Urgent Patient Guidance Centers (CODUs) in digital platforms, later supplemented and transcribed by rescue teams into physical formats, such as paper reports used in ambulances. This coexistence of digital and analog means, coupled with the diversity of involved entities, poses additional challenges to ensuring the confidentiality, integrity, and security of the collected information.

IV. Regulatory Framework

The construction of the current European regulatory framework for the protection of personal and health data reflects a long historical and legal process that has accompanied the technological and social transformations of the continent and the world at large. From the Greek civilizations addressing the need to safeguard intimate aspects, to the consolidation of specific regulations for the processing of data in sensitive sectors such as health, European law has evolved to respond to the challenges imposed by modernity.

Progress in this domain was marked by the initial adoption of declarations and conventions that established the basic principles of data protection, followed later by directives and regulations that harmonize practices among the European Union Member States. Moreover, legislative and regulatory instruments from the Council of Europe have also played a crucial role in defining minimum protection standards, directly influencing European legislation.

In this regard, Table I presents the main legal instruments currently in force with specific relevance to the health sector at the European level.

TABLE I
European Legal Framework

Year	Title	Description
1948	Universal Declaration of Human Rights [19]	Document recognizing the right to protection against arbitrary interference in private life, marking an initial milestone in the defense of privacy as a human right
1950	European Convention on Human Rights [20]	Treaty guaranteeing the right to respect for private and family life, with specific protection against interference by the State or third parties
1981	Council of Europe Convention 108 [21]	First binding international treaty on data protection, establishing standards for Member States
2000	Charter of Fundamental Rights of the EU [22]	Recognizes the protection of personal data as a fundamental right in Article 8, consolidating its importance in the European legal order
2002	Directive 2002/58/EC [23]	Concerning the processing of personal data and the protection of privacy in electronic communications, also known as the *ePrivacy* Directive
2016	Regulation (EU) 2016/679 (GDPR) [24]	General Data Protection Regulation, directly applicable in all Member States, establishing robust protection standards and rights for data subjects
2021	European Health Data Space Proposal [25]	Initiative by the European Commission to establish a regulatory framework facilitating the secure sharing of health data for care, research, and public policy
2022	Directive 2022/2555 (NIS2) [26]	Focuses on cybersecurity and includes health entities as part of critical sectors required to protect sensitive data against security incidents

National legislation on personal and health data protection stems from the need to ensure information security, confidentiality, and citizen privacy, aligning with European principles while addressing Portugal's specific challenges.

In recent years, Portuguese law has evolved by transposing directives and implementing specific regulations to balance technological innovation and privacy protection.

Table II presents the most relevant legal instruments for Portugal's health sector.

TABLE II
Portuguese Legal Framework

Year	Title	Description
2004	Law No. 41/2004, of August 18 [27]	Regulates data protection in the electronic communications sector, aligned with Directive 2002/58/EC
2005	Law No. 12/2005, of January 26 [28]	Establishes specific rules for the processing of genetic information and health data, focusing on confidentiality and access by authorized personnel
2010	Deliberation 629/2010 by the National Data Protection Commission (CNPD) [29]	Defines rules for the processing of health data by entities outside the health sector, with direct impact on the actions of rescuers and operational personnel in the pre-hospital context
2019	Law No. 58/2019, of August 8 [30]	Implemented the GDPR in Portugal, adapting national legislation to European provisions

In summary, this systematization highlights the progressive legislative effort in defining rights, obligations, and guarantees, reinforcing the importance of legal compliance by entities that daily handle sensitive citizen information.

V. Duties of Professionals and Rights of Victims

After analyzing European and national legislation, it is important to understand how these rules apply to the specific context of pre-hospital emergency care. Although many legal instruments were created with a focus on the health sector, not all apply directly to the operational reality of rescue teams. Some directives address technical areas such as telecommunications or network security, while others establish principles directly relevant to the processing of victims' data.

Despite their diversity, these regulations complement each other and share common foundations such as confidentiality, security, and limitation of data processing. However, the practical application of these principles can raise uncertainties on the ground, where urgency and the variability of situations demand adapted interpretations.

In this regard, Table III summarizes the main legal obligations of emergency professionals, highlighting how legal principles translate into concrete responsibilities.

TABLE III
Duties of Emergency Professionals

Duty	**Legal Basis**
Request the victim's consent	Art. 8 Charter of Fundamental Rights, Art. 6 GDPR, Art. 16 Law no. 58/2019
Maintain professional secrecy	Arts. 9 and 90 GDPR, Art. 29 Law no. 58/2019
Report incidents	Arts. 33 and 34 GDPR, Art. 23 NIS2 Directive
Collect data lawfully	Art. 5 Convention 108, Art. 5 GDPR
Limit data collection purposes	Arts. 5, 13, 14 and 15 GDPR, Art. 3 Law no. 12/2005, Art. 23 Law no. 58/2019
Minimize data collected	Arts. 5, 25 and 47 GDPR
Keep data up to date	Art. 5 GDPR, Art. 4 EHDS Proposal
Limit data retention	Art. 5 GDPR, Art. 21 Law no. 58/2019
Ensure data integrity and security	Art. 7 Convention 108, Arts. 5 and 32 GDPR, Art. 29 Law no. 58/2019
Protect data when the victim is unconscious	Art. 9 GDPR
Avoid processing sensitive data	Art. 6 Convention 108, Art. 9 GDPR
Use clear and accessible language	Arts. 7 and 12 GDPR
Provide information about the victim's condition	Art. 8 Convention 108, Art. 8 Charter of Fundamental Rights, Art. 3 Law no. 12/2005, Art. 15 GDPR, Art. 3 EHDS Proposal
Rectify data upon request	Art. 8 Convention 108, Art. 8 Charter of Fundamental Rights, Arts. 5, 15, 16 and 19 GDPR, Art. 17 Law no. 58/2019
Delete data upon request	Art. 8 Convention 108, Arts. 5 and 17 GDPR, Art. 17 Law no. 58/2019
Provide justification for data processing	Art. 8 Convention 108, Art. 3 EHDS Proposal, Art. 3 Law no. 12/2005, Arts. 12, 13 and 15 GDPR, Art. 17 Law no. 58/2019
Assess risks and impacts	Arts. 3, 35 and 36 GDPR, Art. 7 Law no. 58/2019
Adopt privacy and confidentiality measures	Arts. 5, 28 and 32 GDPR, Art. 29 Law no. 58/2019
Destroy or anonymize data for other purposes	Arts. 17 and 89 GDPR, Arts. 21 and 31 Law no. 58/2019
Ensure communication security	Art. 5 Directive 2002/58/EC, Art. 32 GDPR, Art. 17 Law no. 58/2019
Cooperate with the supervisory authority	Art. 31 GDPR, Art. 8 Law no. 58/2019
Prove that consent was given	Arts. 7 and 28 GDPR, Art. 21 Law no. 58/2019
Inform about the right to withdraw consent	Arts. 7 and 13 GDPR, Art. 37 Law no. 58/2019

This diversity of duties reflects the complexity of the legal framework applied to pre-hospital emergency care, highlighting the need for adequate training and continuous updates to ensure compliance with the rules without compromising the effectiveness of emergency response or exposing professionals to potential legal or disciplinary consequences.

In addition to being aware of their legal obligations, those responsible for data processing may benefit from a broader understanding by also analysing the rights of the victims. These rights not only justify many of the obligations imposed on professionals, but also reinforce the need to ensure that any information processing is carried out in a transparent and secure manner.

It is important to note that all professional duties translate, either directly or indirectly, into rights for data subjects; however, Table IV focuses only on those rights that have not already been reflected in the table of duties, thus avoiding redundancies and highlighting complementary aspects of the legal protection afforded to victims.

TABLE IV
Additional Rights of Victims

Right	**Legal Basis**
Respect for private and family life	Art. 12 UDHR, Art. 8 ECHR, Art. 7 EU Charter of Fundamental Rights
Make emergency calls with confidentiality	Art. 5 Directive 2002/58/EC, Art. 14 Law No. 41/2004, Art. 32 GDPR, Art. 17 Law No. 58/2019
Lodge a complaint with the supervisory authority	Arts. 12, 13, 14 and 15 GDPR
Have their data protected after death	Art. 17 Law No. 58/2019
Grant rights to heirs	Art. 17 Law No. 58/2019
Be compensated by the controller for damages	Art. 33 GDPR
Not be subject to automated decisions	Art. 22 GDPR
Know who accessed their data	Art. 3 EEDS Proposal, Art. 29 Law No. 58/2019

The variety of rights once again reflects the complexity of the legal framework governing data processing in healthcare, underlining the need for emergency teams not only to be aware of their obligations, but also to understand and respect the rights of victims.

In addition to rights, the victims also have fundamental duties that contribute to the proper functioning of the emergency response system. Among these are the responsibility to provide accurate and complete information to rescuers and to respect the rights and instructions of emergency teams.

Finally, it should be emphasized that, in situations not expressly addressed in Tables III and IV, professionals must always ensure a balance between protecting the victim's privacy and safeguarding their life condition, ensuring that any processing of personal data complies with the fundamental principles of privacy and security.

VI. Case Study

In addition to the normative analysis and its translation into practical principles, this study also sought to assess the procedures and level of awareness among emergency professionals regarding data protection. To this end, a case study was carried out, understood as an approach focused on the in-depth analysis of a specific reality, with the aim of understanding practices, identifying challenges, and proposing improvements [31].

This method proves particularly relevant in the pre-hospital emergency context, where the application of legal norms requires constant adaptation to the field. Direct observation of practices helps complement the theoretical perspective, contributing to a more realistic view of how legal obligations are applied and the obstacles faced by emergency teams.

A. Methodology

To ensure the validity and reliability of the study, a preliminary exploratory analysis was conducted across various academic databases, in search of existing assessment instruments concerning data protection in medical emergency contexts. However, no questionnaires specifically tailored to the pre-hospital domain were found, which justified the development of an original instrument.

A clear definition of the methodological strategy not only ensures the coherence and objectivity of the study, but also guarantees that the adopted procedures are replicable and suited to the context under analysis. In this case, the adopted strategy followed a structured set of phases:

1) **Identification of the objectives** to be achieved;
2) **Design of the questionnaire**, ensuring the effective collection of relevant responses;
3) **Distribution of the questionnaire**, using appropriate channels to reach different categories of professionals;
4) **Collection of results** in an anonymous and organized manner;
5) **Analysis of the responses** to identify trends, patterns, and discrepancies in the collected data;
6) **Discussion** and drawing of conclusions.

Given the objective of this stage, a quantitative method was adopted for data analysis—a widely recognized approach for its capacity to measure and quantify social phenomena in an objective and systematic way. This methodology was chosen as it enables the collection and analysis of numerical data, providing a clear view of the frequency and distribution of certain attitudes, behaviours, or opinions among pre-hospital emergency professionals. Furthermore, this method facilitates the generalization of results from a representative sample, ensuring greater statistical rigor and validity [32].

1) Data Collection Instrument: For data collection, electronic questionnaires were used, given their effectiveness in obtaining responses in a practical, anonymous, and confidential manner. The instrument was developed and administered using the Microsoft Forms platform, chosen for its simplicity, accessibility, and compliance with legal principles of anonymity and information security.

2) Questionnaire Structure: The participant approach begins with an introductory message that clarifies the study's objectives and academic context, while assuring participants of anonymity, voluntary participation, and the possibility to withdraw at any time. In addition, the average completion time and a contact email for any questions are also provided. The questionnaire was structured into five sections, organized logically and sequentially to facilitate understanding and the systematic collection of information:

1) **Consent:** The participant confirms their agreement to take part in the study, accepting to do so voluntarily, freely, and with informed understanding;
2) **Sociodemographic Characterization:** Basic information is collected about the participants' profile, including gender, age group, educational background, region, years of service, and institutional affiliation;
3) **Perception of Current Legislation:** Professionals' general perception of data protection legislation is assessed through questions about their familiarity with key legal concepts, as well as whether they have attended any training in the area and how long ago it occurred;
4) **Practical Assessment:** An analysis is conducted on the professionals' practical knowledge of legal obligations concerning data processing during the provision of care. It includes questions on consent procedures, data transmission security, access to information, and communication with journalists and police authorities;
5) **Challenges and Improvements:** Participants are asked to identify the main difficulties encountered in the field. Furthermore, they are invited to suggest the main improvements they consider necessary to strengthen data protection in the sector.

At the level of internal composition, all sections consist exclusively of structured, closed-format questions, predominantly multiple-choice, where one or more answers are correct and the others incorrect.

3) Questionnaire Pre-Test: Prior to its dissemination, the questionnaire underwent a pre-test with four pre-hospital emergency professionals, selected for having diverse profiles in

terms of affiliation, training, age, and years of service. This diversity enabled the collection of feedback representative of different operational realities. The participants completed the entire questionnaire and then assessed the clarity, relevance, and coherence of the questions, as well as the language, duration, and level of difficulty, contributing to the practical validation and final adjustment of the instrument. Based on the reviewers' feedback, minor modifications were made to the questionnaire.

In addition to the qualitative analysis of the reviewers' opinions, it is also relevant to observe their responses to the questionnaire, as this offers a preliminary insight into potential trends and helps gauge the level of awareness that a broader sample of professionals might demonstrate. From the answers given in the practical scenarios section, approximately 61% were correctly selected by the reviewers, suggesting that although there is some practical understanding of certain principles, several weaknesses still persist.

4) Dissemination Strategy: Finally, it was essential to ensure that data collection was carried out effectively through a well-planned dissemination strategy. This step is of particular importance, as the quality of the results depends directly on the ability to reach a representative number of professionals, ensuring diversity and reliability within a convenience sample.

Accordingly, the approach adopted aimed to maximize the questionnaire's reach within the emergency and rescue community, using various communication channels to encourage participation and ensure sample representativeness:

- **Email communication**, directed to institutional contacts capable of promoting internal sharing among their staff;
- **Social media**, through posts and shares in professional groups on platforms such as Facebook, Telegram, and WhatsApp;
- **Direct communication** with professionals in the field, using the author's personal network established through his role as a Volunteer Firefighter.

The questionnaire remained available for a period of three weeks, during which follow-up messages and periodic reminders were sent to encourage continued participation and reinforce engagement among potential respondents who had not yet completed it.

B. Results

During the planned period, the questionnaire collected 143 valid responses, exceeding initial expectations due to the extensive dissemination strategy implemented. The average completion time was 13.17 minutes, slightly above the estimated 10 minutes, suggesting participants were committed when providing their answers.

For the analysis, the statistical panel of Microsoft Forms was used, along with the exportation of an Excel file containing all individual responses, allowing for a more detailed data treatment. To identify trends and general perceptions, simple descriptive analyses were conducted—such as means, percentages, and frequencies—without any individualized analysis, thus safeguarding anonymity.

1) Sample Characterization: Regarding gender, 64% of participants identified as male. The most represented age group was 41–50 years (37%), followed by 21–30 years (28%) and 31–40 years (22%).

In terms of education level, 55% of respondents had completed secondary education, 25% held a bachelor's degree, 8% reported having a technical specialization course, and 7% had completed a master's degree.

Geographically, 47% of responses came from the Central region, 20% from Lisbon and the Tagus Valley, 20% from the North, 7% from the Algarve, and 6% from the Alentejo.

Concerning length of service, 26% had more than 25 years of experience, 25% had less than 5 years, 18% had between 16–20 years, 16% between 11–15 years, and 15% between 6–10 years.

Finally, institutional affiliation was distributed among 53% professionals and 47% volunteers. Regarding the roles performed, 58% were emergency ambulance crew members, 27% were non-emergency transport crew, 11% held other roles, and 3% were nurses or emergency technicians.

2) Perception of Legislation: When asked about their knowledge of European regulations and national legislation on data protection, 67 participants (47%) stated that they are aware of the current legislation, 12 (8%) indicated that they are completely unaware of it, and 63 (44%) reported having only partial knowledge.

The following question aimed to understand whether respondents had attended specific training in data protection. Of the 143 participants, 54 (38%) stated they had received training within the last five years, 13 (9%) indicated that this training occurred more than five years ago, 36 (25%) declared they had never had any training, and 39 (27%) said that, although they never had training, they would like to attend it.

Regarding the place where the training was obtained, the results showed that, among the 67 participants who stated they had received training, the majority—32 responses (48%)—indicated that this training was provided by an entity external to their institution. Meanwhile, 26 responses (39%) said the training was offered internally by the institution where the participant works. Finally, only 9 participants (13%) reported acquiring this knowledge through personal initiative and interest.

Lastly, when asked about the distinction between personal data and sensitive data, 84 respondents (59%) said they did not know how to distinguish or were unsure about this difference.

3) Awareness in Practical Scenarios: Based on the overall analysis of the responses obtained in the scenario-based questions, an average error rate of approximately 56% was observed. Despite being professionals with direct experience in emergency response and regular contact with personal and sensitive data, more than half were unable to correctly apply legal principles in simulated real-life situations.

Questions related to the identification of special categories of data (error rate of 61%), providing information to family members (error rate of 72%), demonstrating the collection of consent (error rate of 80%), and dealing with journalists

(error rate of 58%) proved particularly challenging for many respondents.

Among the most correctly answered questions were those regarding the information to be provided to the victim before data collection (79% correct), the destruction of notes after the incident (61% correct), and the sharing of information with law enforcement authorities (56% correct).

4) Challenges and Improvements: In the final section of the questionnaire, the main obstacles faced by professionals in complying with legal standards were identified, along with suggestions to improve data protection in the pre-hospital emergency context.

The most frequently mentioned challenge, with 104 responses, was the need for specific training on data protection, reflecting the previously evidenced skills gap. Secondly, 89 participants highlighted the lack of uniform procedures for recording consent. The complexity and fragmentation of applicable legislation was referred to by 62 respondents as a barrier to its correct understanding and application in the field.

In addition to these, other challenges received considerable attention, namely the difficulty in ensuring confidentiality in public places, the lack of mechanisms/resources for managing and preserving information post-event, and the conflict between legal principles and the need to share information with hospitals and authorities.

Regarding proposed improvements, the most voted measure was the creation of a simplified practical guide (101 responses), followed by the implementation of continuous and mandatory training (100 responses). The third most mentioned measure, with 93 responses, was the establishment of clear protocols for recording consent, demonstrating the urgency for objective and uniform tools to support professionals' actions.

The less voted suggestions relate to the appointment of Data Protection Officers in Fire Departments and Red Cross Delegations, the provision of secure communication devices such as service mobile phones, and the creation of regular internal audits and inspections to monitor and support compliance with the regulations.

VII. Discussion

Despite significant and representative participation, the data obtained reveal notable weaknesses in the practical knowledge of the current legislation. The average score achieved on the practical scenario questions—those that most directly assess the concrete application of legal principles in real emergency contexts—was only 4.4 out of 10.

The results confirm gaps already identified in the literature, which highlight specific difficulties in the pre-hospital environment, such as the complexity of regulations, lack of specific training, absence of clear procedures, and challenges in maintaining confidentiality in public spaces. The fragmented legislation and scarcity of targeted materials increase professionals' uncertainty.

In response, the adoption of good practices for recording consent and physical security measures is recommended, along with regular, practical, and contextualized training, the use of communication devices dedicated to the service, as well as the availability of quick-reference guides and auditing mechanisms. It is also suggested to improve official documents, such as the emergency report, to include explicit fields on consent and reinforce confidential document labeling. Finally, the creation of a practical guide, developed in this study, is emphasized, which gathers essential norms in a simple and accessible manner, facilitating safe and legally informed action by professionals in the field.

These measures aim to mitigate the challenges faced, promoting safer and more compliant conduct with data protection legislation in the pre-hospital context.

VIII. Conclusions

This work resulted in the production of a unique and accessible document that compiles and clarifies the applicable legal framework, promoting a better understanding of citizens' rights and the obligations of emergency professionals. It also contributed to identifying the level of awareness among professionals and the main challenges in the practical application of legislation. From a scientific perspective, the originality of the study stands out, as it addresses a still underexplored area, providing relevant data for future research and practice. The investigation also allowed the author to gain significant in-depth knowledge of the legal aspects of data protection, with a direct impact on their academic training and professional performance.

Among the obstacles encountered, the scarcity of specific bibliography and the complexity of dispersed legislation stand out, as well as methodological challenges in the questionnaire design and the technical translation of legal content. Nevertheless, the study was successfully conducted.

The reliance on convenience sampling and the absence of validated instruments constrain the generalizability of the findings, underscoring the importance of continued and more robust research efforts. The need for continuous and more robust future research is acknowledged.

Among the suggested improvements are strengthening the literature review, optimizing the questionnaire, broadening the sample, and exploring the possibility of forensic analyses on digital systems used in emergency operations.

Thus, the work meets its proposed objectives and constitutes a relevant contribution to the debate on data protection in emergency contexts.

Acknowledgment

The author would like to thank all the professionals who participated in the study and contributed with their time and insights.

This research was supported by FCT Pluriannual Funding UID/308, through the Instituto de Engenharia de Sistemas e Computadores de Coimbra – INESC Coimbra.

References

[1] Morgado, L. (Dec. 27, 2024). Literature Reviews integrating AI tools. (Accessed in the jan. 20, 2025). URL: https://repositorioaberto.uab.pt/entities/publication/17f5ba74-c46d-4aa2-93a8-b8603102d2ea

[2] Carvalho, C. (Mar. 2022). A Proteção de Dados Pessoais de Saúde. (Accessed in the dec. 10, 2024). URL: https://iconline.ipleiria.pt/handle/10400.8/8824

[3] Nunes, G. (Jun. 2019). O tratamento de dados pessoais de saúde à luz do regulamento geral europeu de proteção de dados pessoais. (Accessed in the dec. 10, 2024). URL: https://estudogeral.sib.uc.pt/handle/10316/89580

[4] Tinto, A. (Aug. 2018). Protecção de dados de saúde Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia. (Accessed in the dec. 10, 2024). URL: https://run.unl.pt/handle/10362/58821

[5] SPMS, EPE. (n.d.). Privacidade da Informação no setor da Saúde. (Accessed in the dec. 30, 2024). URL: https://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

[6] INEM et al. (Mar. 2024). Curso TAS: Tripulante de Ambulância de Socorro. (Accessed in the nov. 23, 2024). URL: https://aprender.inem.pt/pluginfile.php/358741/mod_resource/content/2/MANUAL_TAS_V1_MAR24.pdf

[7] Koskimies, E., Koskinen, S., Leino-Kilpi, H., and Suhonen, R. (Sep. 5, 2020). The informational privacy of patients in prehospital emergency care — Integrative literature review. (Accessed in the jan. 15, 2025). URL: https://research.utu.fi/converis/portal/detail/publication/49029347

[8] Mitra, A., Gochhait, S., Obaid, A., and Alkhafaji, M. (2023). A Strategic Data Protection Plan for the Healthcare Industry-A Review. (Accessed in the jan. 22, 2025). URL: https://ieeexplore.ieee.org/document/10192830

[9] Yeng, P., Yang, B., and Snekkenes, E. (2019). Framework for Healthcare Security Practice Analysis, Modeling and Incentivization. (Accessed in the jan. 23, 2025). URL: https://ieeexplore.ieee.org/document/9006529

[10] Singh, G., Tiwari, D., Goel, P., Vishwakarma, P., Gupto, K., and Verma, A. (2024). Cybersecurity Challenges In Healthcare Systems. (Accessed in the jan. 23, 2025). URL: https://ieeexplore.ieee.org/document/10593022

[11] Shingari, N., Verma, S., Mago, B., and Javeid, M. (2023). A review of cybersecurity challenges and recommendations in the healthcare sector. (Accessed in the jan. 23, 2025). URL: https://ieeexplore.ieee.org/document/10111096

[12] Geiderman, J., Moskop, J., and Derse, A. (2006). Privacy and Confidentiality in Emergency Medicine: Obligations and Challenges. (Accessed in the jan. 24, 2025). URL: https://www.sciencedirect.com/science/article/pii/S0733862706000332

[13] Moskop, J., Marco, C., Larkin, G., Geiderman, J., and Derse, A. (2005). From Hippocrates to HIPAA: Privacy and confidentiality in Emergency Medicine—Part II: Challenges in the emergency department. (Accessed in the jan. 28, 2025). URL: https://www.sciencedirect.com/science/article/pii/S019606440401282X

[14] Erbay, H. (2014). Some Ethical Issues in Prehospital Emergency Medicine. (Accessed in the jan. 24, 2025). URL: https://www.sciencedirect.com/science/article/pii/S2452247316300747

[15] Koskimies, E., Koskenniemi, J., and Leino-Kilpi, H. (2019). Patient's informational privacy in prehospital emergency care: Paramedics' perspective. (Accessed in the jan. 26, 2025). URL: https://journals.sagepub.com/doi/10.1177/0969733019834977

[16] INEM. (Nov. 23, 2020). Gestos que salvam! – Quais os Critérios do INEM para Enviar Meios de Socorro. (Accessed in the nov. 22, 2024). URL: https://www.inem.pt/2020/11/23/gestos-que-salvam-quais-os-criterios-do-inem-para-enviar-meios-de-socorro-5/

[17] M. Alexandre. (Jun. 20, 2023). Qual a importância do atendimento pré-hospitalar? (Accessed in the jun. 10, 2025). URL: https://vidasaudavel.einstein.br/qual-a-importancia-do-atendimento-pre-hospitalar/

[18] INEM. (Feb. 11, 2024). Mais de 1.5 milhões de chamadas de emergência atendidas nos CODU do INEM em 2023. (Accessed in the nov. 14, 2024). URL: https://www.inem.pt/2024/02/11/mais-de-1-5-milhoes-de-chamadas-de-emergencia-atendidas-nos-codu-do-inem-em-2023/

[19] United Nations. (n.d.). Universal Declaration Of Human Rights. (Accessed in the nov. 14, 2024). URL: https://unric.org/en/human-rights-75/

[20] Conselho da Europa. (n.d.). Convenção Europeia dos Direitos do Homem. (Accessed in the jan. 12, 2025). URL: https://www.echr.coe.int/documents/d/echr/Convention_POR

[21] Conselho da Europa. (Jan. 28, 1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Accessed in the jan. 12, 2025). URL: https://www.coe.int/en/web/data-protection/convention108-and-protocol

[22] United Nations. (Oct. 26, 2012). Charter of Fundamental Rights of the European Union. (Accessed in the jan. 12, 2025). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[23] United Nations. (Jul. 12, 2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). (Accessed in the jan. 12, 2025). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058

[24] United Nations. (Apr. 27, 2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (Accessed in the jan. 12, 2025). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[25] United Nations. (May 3, 2022). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space. (Accessed in the jan. 13, 2025). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

[26] United Nations. (Dec. 14, 2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). (Accessed in the jan. 13, 2025). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[27] Assembleia da República. (Aug. 18, 2004). Lei n.º 41/2004, de 18 de agosto. (Accessed in the jan. 12, 2025). URL: https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710

[28] Assembleia da República. (Jan. 26, 2005). Lei n.º 12/2005, de 26 de janeiro. (Accessed in the jan. 12, 2025). URL: https://diariodarepublica.pt/dr/detalhe/lei/12-2005-624463

[29] Roque, A., Lobo, C., Andrade L., António H., Barroso, L., Almeida, V., and Silveira, L. (Sep. 13, 2010). Deliberação n.º 629/2010: Princípios aplicáveis ao tratamento de dados de gravação de chamadas. (Accessed in the jan. 12, 2025). URL: https://www.cnpd.pt/media/q01alptr/del629_2010.pdf

[30] Assembleia da República. (Aug. 8, 2019). Lei n.º 58/2019, de 8 de agosto. (Accessed in the jan. 13, 2025). URL: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

[31] Hollweck, T. (2015). Robert K. Yin.(2014). Case Study Research Design and Methods. (Accessed in the mar. 11, 2025). URL: https://utppublishing.com/doi/pdf/10.3138/cjpe.30.1.108

[32] Grand Canyon University. (Oct. 9, 2023). Qualitative vs. Quantitative Research: What's the Difference? (Accessed in the jun. 10, 2025). URL: https://www.gcu.edu/blog/doctoral-journey/qualitative-vs-quantitative-research-whats-difference