UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

PROTEÇÃO DE DADOS PESSOAIS EM SAÚDE E HOSPITAIS E.P.E.: RESPONSABILIDADE CIVIL DO RESPONSÁVEL PELO TRATAMENTO

Diogo Miguel Alcaçarenho Rosa

MESTRADO PROFISSIONALIZANTE

CIÊNCIAS JURÍDICO-EMPRESARIAIS

Lisboa, 19 de julho de 2018

UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

PROTEÇÃO DE DADOS PESSOAIS EM SAÚDE E HOSPITAIS E.P.E.: RESPONSABILIDADE CIVIL DO RESPONSÁVEL PELO TRATAMENTO

Diogo Miguel Alcaçarenho Rosa

MESTRADO PROFISSIONALIZANTE

CIÊNCIAS JURÍDICO-EMPRESARIAIS

Orientadora: Professora Doutora Ana Perestrelo de Oliveira

Agradecimentos

Neste e noutros desafios da minha vida, não posso nunca deixar de agradecer à minha família, sem distinções, pelas condições proporcionadas e pelo apoio incondicional que me é dado. Um simples e sentido obrigado, será por vezes a mais reconhecida homenagem.

Resumo

A presente dissertação de mestrado do curso de Mestrado em Ciências Jurídico-Empresariais da Faculdade de Direito da Universidade de Lisboa tem como principal objetivo abordar a temática da proteção de dados pessoais em saúde, bem como a problemática da responsabilidade extracontratual delitual por violação de dados pessoais, nomeadamente atendendo à realidade dos Hospitais e Centros Hospitalares E.P.E., por serem as instituições de saúde mais representativas na prestação de cuidados de saúde aos utentes do Serviço Nacional de Saúde.

No âmbito do presente estudo, temos a oportunidade de realizar uma abordagem inicial à problemática da proteção de dados pessoais em saúde, atendendo à dimensão das estruturas hospitalares e do tipo de dados pessoais tratados, bem como das operações de tratamento a que esses dados em saúde são sujeitos.

Realizamos ainda um breve apontamento sobre a constituição interna dos Hospitais E.P.E., com o objetivo de compreender melhor a complexidade organizacional daquelas instituições e as competências dos seus órgãos.

Realizamos um enquadramento sobre o Regulamento Geral de Proteção de Dados da União Europeia 2016/679, tocando nos seus conceitos, nos princípios de tratamento de dados, no tratamento de dados pessoais em saúde, no Encarregado de Proteção de Dados, nos registos das atividades de tratamentos e também na autoridade nacional de controlo em matéria de proteção de dados, não sem antes nos referirmos à atual lei de proteção de dados pessoais, a Lei n.º 67/98, de 26 de outubro.

Numa fase final, abordamos o regime da responsabilidade civil extracontratual do Estado por violação de dados pessoais em saúde, tocando neste aspeto como uma das mais graves consequências para estas instituições em caso de violação de dados pessoais, dando exemplos práticos, que pretendem demonstrar qual é a realidade e as eventuais fragilidades dos Hospitais e Centros Hospitalares E.P.E. em Portugal.

Por último, e após a identificação da problemática, propomos medidas com vista à mitigação dos riscos de Violação de Dados Pessoais, procurando apresentar algumas medidas internas que as instituições podem adotar, no sentido de cumprir com o princípio da responsabilidade demonstrável no âmbito dos tratamentos de dados efetuados, nomeadamente a implementação de um sistema de gestão de dados pessoais com medidas para constituição de equipa afeta à implementação do Sistema de Gestão de Dados, Realização de Diagnóstico e Avaliação do Hospital, Nomeação do Encarregado de Proteção de Dados, Designação de Responsável do Acesso à Informação, Planeamento da implementação e execução e desenho do Governo do Sistema de Gestão de Dados Pessoais.

Palavras-chave: Proteção de Dados, Dados em Saúde, Privacidade, Hospital, Centro Hospitalar, Entidade Pública Empresarial, E.P.E., Responsabilidade Civil Extra Contratual do Estado

Abstract

This M.Sc. Dissertation, on the scientific area of masters degree in corporate law, aims primarily to explore the problem of data protection in healthcare systems, as well as *State's "extra contractual" civil responsibility regarding personal data protection violations in public healthcare*, *taking into particular account the reality of "Hospitals and Hospital Centers E.P.E.", as the most representative healthcare institutions in the Portuguese National Healthcare Service.*

In the context of this study, we present an initial exploration of the issue of data protection in healthcare, taking into account the dimension of the healthcare institution, the kinds of personal data that are employed, as well as the treatment that that data is subject to while in the system.

We also broach the subject of the internal organization of "Hospitals E.P.E.", aiming to better understand the organizational complexity of these institutions, as well as the individual tasks of the components of their management structure.

We present the European Union's General Data Protection Regulation (2016/679, transposed into national Law Nº 67/98), detailing its main concepts, data protection principles, specific regulations regarding data protection in healthcare, the concept of Data Protection Officer, the national authority for data protection, and analyze them with respect to the necessary logging of healthcare practices.

Ending the study of the problem matter, we will detail the State's "extra contractual" civil responsibility regarding personal data protection violations in public healthcare, which constitutes one of the gravest consequences for these institutions in cases of data protection violation. We provide practical examples demonstrating the Portuguese reality and the main possible weaknesses of the systems implemented in "Hospitals and Hospital Centers E.P.E.".

Lastly, having properly defined and detailed the problem at hand, we will propose measures aiming to mitigate the risks of data protection violation, presenting internal policies that institutions can adopt towards aligning themselves with the principles of demonstrable responsibility in the context of healthcare. These measures are mainly composed of implementation of a personal data management system, by building an implementation team of the Data Management System, Diagnostic and Evaluation of the Hospital, Appointment of the Data Protection Officer, designation of the Responsible for Information Access, Planning implementation and execution and design of the Government Personal Data Management System.

Keywords: *Data Protection, Healthcare Data, Privacy, Hospital, Hospital Center, Corporate Public Entity, E.P.E., State's "extra contractual" civil responsibility*

Siglas e Abreviaturas

AC.	Acórdão
AIP	Avaliação de Impacto sobre a Proteção de Dados
ADC	Autoridade de Controlo
ACSS	Administração Central do Sistema de Saúde, I.P.
ARS	Administração Regional de Saúde, I.P.
CA	Conselho de Administração
CADA	Comissão de Acesso aos Documentos Administrativos
CC	Código Civil
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
CNCS	Centro Nacional de Cibersegurança
DL	Decreto-Lei
E.P.E.	Entidade Pública Empresarial
EPD	Encarregado de Proteção de Dados
ERS	Entidade Reguladora da Saúde
GT29	Grupo de Trabalho do Artigo 29
LPD	Lei Proteção de Dados
RAI	Responsável do Acesso à Informação
RGPD	Regulamento Geral de Proteção de Dados
ROC	Revisor Oficial de Contas
SNS	Serviço Nacional de Saúde
SS	Seguintes
SGMS	Secretaria-Geral do Ministério da Saúde

SPMS Serviços Partilhados do Ministério da Saúde

TC Tribunal Constitucional

TR Tribunal da Relação

UE União Europeia

Índice

Introdução

A presente dissertação de mestrado, do Curso de Mestrado em Ciências Jurídico-Empresariais da Faculdade de Direito da Universidade de Lisboa, tem como principal objetivo abordar a temática da Proteção de Dados Pessoais relativos à saúde, em particular a proteção de dados pessoais dos Hospitais e Centros Hospitalares E.P.E., e atender à problemática da responsabilidade civil do responsável pelo tratamento nas diferentes variáveis por violação da proteção de dados pessoais, nomeadamente de dados pessoais em saúde.

O nosso estudo atenderá às disposições constantes no direito interno português e no direito da União Europeia, tendo como finalidade a apresentação de soluções que possam mitigar esta problemática e proteger as instituições para a eventualidade da violação de dados dos seus utentes e colaboradores, à luz do Novo Regulamento Geral de Proteção de Dados EU 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.[1]

Neste sentido, pretendo com o presente estudo efetuar uma abordagem inicial sobre o direito fundamental de proteção da saúde, direito consagrado na Constituição da República Portuguesa em paralelo com o direito à reserva da intimidade da vida privada, fazendo ainda uma referência acerca do Serviço Nacional de Saúde em Portugal.

Considero ainda imprescindível que seja efetuada uma abordagem à Lei n.º 67/98, de 26 de outubro, a Lei da Proteção Dados Pessoais que transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, 24/10/95[2], relativa à proteção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados e que, ao momento presente, ainda se encontra em vigor.

[1] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[2] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

No âmbito do presente estudo, considero também importante que seja explicada a constituição dos Hospitais e Centros Hospitalares pertencentes ao setor público empresarial do Estado, uma vez que estas entidades, com autonomia patrimonial e financeira, revestem a grande maioria das instituições prestadoras de cuidados de saúde em Portugal, tendo sido realizada uma clara distinção entre a constituição formal e funções de cada órgão pertencente a este tipo de organismos, por forma a que, no desenrolar do nosso estudo, fossem mais facilmente enquadráveis as soluções propostas aos problemas que fossem sendo identificados.

Neste âmbito, importa contabilizar aqueles que são os Hospitais e Centros Hospitalares E.P.E. no nosso país, em paralelo com outras instituições de saúde com outra natureza jurídica, nomeadamente de acordo com os dados disponíveis no sítio da internet do Serviço Nacional de Saúde.

Assim, de acordo com a informação disponibilizada naquele sítio da internet, existem em Portugal as seguintes instituições de saúde, pertencentes ao **Setor Público Empresarial**[3]:

- Instituto Português de Oncologia de Lisboa Francisco Gentil (IPO);
- Unidade Local de Saúde de Castelo Branco, EPE;
- Unidade Local de Saúde de Matosinhos, EPE;
- Unidade Local de Saúde do Alto Minho, EPE;
- Unidade Local de Saúde da Guarda, EPE;
- Unidade Local de Saúde do Baixo Alentejo, EPE;
- Unidade Local de Saúde do Litoral Alentejano, EPE;
- Unidade Local de Saúde do Norte Alentejano, EPE;
- Unidade Local de Saúde do Nordeste, EPE;
- Centro Hospitalar do Porto, EPE;
- Centro Hospitalar de Entre Douro e Vouga, EPE;
- Centro Hospitalar de Trás-os-Montes e Alto Douro, EPE;
- Hospital da Senhora da Oliveira Guimarães, EPE;
- Centro Hospitalar do Médio Ave, EPE;
- Centro Hospitalar de S. João, EPE;
- Centro Hospitalar Póvoa de Varzim/Vila do Conde, EPE;
- Centro Hospitalar Tâmega e Sousa, EPE;
- Centro Hospitalar de Vila Nova de Gaia/Espinho, EPE;
- Centro Hospitalar Tondela Viseu, EPE;
- Centro Hospitalar Leiria, EPE;

[3] Retirado de https://www.sns.gov.pt/institucional/entidades-de-saude/

- Centro Hospitalar e Universitário de Coimbra, EPE;
- Centro Hospitalar Cova da Beira, EPE;
- Centro Hospitalar Médio Tejo, EPE;
- Centro Hospitalar Barreiro Montijo, EPE;
- Centro Hospitalar de Lisboa Norte, EPE;
- Centro Hospitalar de Lisboa Ocidental, EPE;
- Centro Hospitalar de Setúbal, EPE;
- Centro Hospitalar Universitário do Algarve, EPE;
- Centro Hospitalar do Baixo Vouga, EPE;
- Centro Hospitalar Lisboa Central, EPE;
- Hospital de Magalhães Lemos, EPE;
- Hospital Santa Maria Maior, EPE – Barcelos;
- Hospital Distrital Figueira da Foz, EPE;
- Instituto Português de Oncologia de Coimbra Francisco Gentil (IPO), EPE;
- Hospital de Santarém, EPE;
- Hospital Garcia de Orta, EPE;
- Hospital Professor Doutor Fernando Fonseca, EPE;
- Instituto Português de Oncologia do Porto Francisco Gentil (IPO), EPE;
- Hospital Espírito Santo, EPE – Évora.

Em paralelo, e apenas a mero título de referência, existem os seguintes **hospitais do Setor Público Administrativo**[4], os seguintes:

- Centro de Medicina Física de Reabilitação do Sul – São Brás de Alportel;
- Centro Hospitalar Psiquiátrico de Lisboa;
- Centro Hospitalar Oeste;
- Centro de Medicina de Reabilitação da Região Centro – Rovisco Pais;
- Hospital Arcebispo João Crisóstomo – Cantanhede;
- Hospital Dr. Francisco Zagalo – Ovar;
- Instituto de Oftalmologia Dr. Gama Pinto.

São ainda **Serviços Desconcentrados das Administrações Regionais de Saúde**, os seguintes:

- Agrupamento de Centros de Saúde Almada-Seixal;
- Agrupamento de Centros de Saúde Amadora;
- Agrupamento de Centros de Saúde Arco Ribeirinho;

[4] Retirado de https://www.sns.gov.pt/institucional/entidades-de-saude/

- Agrupamento de Centros de Saúde Arrábida;
- Agrupamento de Centros de Saúde Cascais;
- Agrupamento de Centros de Saúde Estuário do Tejo;
- Agrupamento de Centros de Saúde Lezíria;
- Agrupamento de Centros de Saúde Baixo Alentejo;
- Agrupamento de Centros de Saúde Baixo Vouga;
- Agrupamento de Centros de Saúde Lisboa Central;
- Agrupamento de Centros de Saúde Lisboa Norte;
- Agrupamento de Centros de Saúde Lisboa Ocidental e Oeiras;
- Agrupamento de Centros de Saúde Loures-Odivelas;
- Agrupamento de Centros de Saúde Médio Tejo;
- Agrupamento de Centros de Saúde Oeste Norte;
- Agrupamento de Centros de Saúde Oeste Sul;
- Agrupamento de Centros de Saúde Sintra;
- Agrupamento de Centros de Saúde de Trás-os-Montes – Alto Tâmega e Barroso;
- Agrupamento de Centros de Saúde do Douro I – Marão e Douro Norte;
- Agrupamento de Centros de Saúde do Douro II – Douro Sul;
- Agrupamento de Centros de Saúde do Alto Ave;
- Agrupamento de Centros de Saúde do Ave – Famalicão;
- Agrupamento de Centros de Saúde do Cávado I – Braga;
- Agrupamento de Centros de Saúde do Cávado II – Gerês/Cabreira;
- Agrupamento de Centros de Saúde do Cávado III – Barcelos/Esposende;
- Agrupamento de Centros de Saúde do Tâmega I – Baixo Tâmega;
- Agrupamento de Centros de Saúde do Tâmega II – Vale do Sousa Sul;
- Agrupamento de Centros de Saúde do Tâmega III – Vale do Sousa Norte;
- Agrupamento de Centros de Saúde do Grande Porto I – Santo Tirso/Trofa;
- Agrupamento de Centros de Saúde do Grande Porto II – Gondomar;
- Agrupamento de Centros de Saúde do Grande Porto III – Maia/Valongo;
- Agrupamento de Centros de Saúde do Grande Porto IV – Póvoa de Varzim/Vila do Conde;
- Agrupamento de Centros de Saúde do Grande Porto V – Porto Ocidental;

- Agrupamento de Centros de Saúde do Grande Porto VI – Porto Oriental;
- Agrupamento de Centros de Saúde do Grande Porto VII – Gaia;
- Agrupamento de Centros de Saúde do Grande Porto VIII – Espinho/Gaia;
- Agrupamento de Centros de Saúde de Entre Douro e Vouga I – Feira/Arouca;
- Agrupamento de Centros de Saúde de Entre Douro e Vouga II – Aveiro Norte;
- Agrupamento de Centros de Saúde da Cova da Beira;
- Agrupamento de Centros de Saúde do Baixo Mondego;
- Agrupamento de Centros de Saúde do Dão – Lafões;
- Agrupamento de Centros de Saúde do Pinhal Interior Norte;
- Agrupamento de Centros de Saúde do Pinhal Litoral;
- Agrupamento de Centros de Saúde do Alentejo Central;
- Agrupamento de Centros de Saúde do Algarve I – Central;
- Agrupamento de Centros de Saúde do Algarve II – Barlavento;
- Agrupamento de Centros de Saúde do Algarve III – Sotavento.

Sendo **Hospitais em parceria público-privada** (PPP), os seguintes:

- Hospital Beatriz Ângelo;
- Hospital de Braga;
- Hospital de Vila Franca de Xira;
- Hospital de Cascais Dr. José de Almeida.

E ainda **Hospitais geridos pelas Misericórdias**, os seguintes:

- Hospital José Hospital S. Paulo – Serpa;
- Hospital Luciano de Castro – Anadia;
- Hospital São José – Fafe.

Para além das instituições de saúde supra mencionadas e identificadas, existem hospitais do setor privado, bem como hospitais das misericórdias e ainda uma panóplia de clínicas, centros médicos, laboratórios de exames e de análises, que bem assim não sendo o objeto principal do nosso estudo, poderão daqui retirar algumas

ideias e seguir alguma da metodologia proposta, no sentido de mitigar eventuais problemáticas ao nível da proteção de dados em saúde, tendo em conta que os dados por tratados por este tipo de instituições têm necessariamente que ser lidados de uma maneira mais cuidada e cumprindo determinados requisitos mais exigentes, como veremos em seguida.

No âmbito do presente estudo, vou analisar a forma como podem as instituições de saúde com carácter de entidade pública empresarial ser civilmente responsabilizadas, nomeadamente por violações das normas instituídas relativamente à proteção de dados pessoais e em específico de dados pessoais relativos à saúde.

Na fase final do nosso estudo, irei propor algumas soluções no sentido de mitigar os riscos no tratamento de dados pessoais, por forma a prevenir as violações de normas instituídas e, por conseguinte, evitar que as instituições incorram em responsabilidade civil nesta matéria, tentando ao mesmo tempo efetuar as propostas à luz do Regulamento Geral sobre a Proteção de Dados (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Por fim, considero pertinente referir que a Proteção de Dados Pessoais é um dos grandes temas do século XXI, que necessita de uma reflexão profunda a nível global e, em particular, no nosso país, sendo certo que os hospitais são das entidades que mais devem adequar o seu funcionamento interno, no sentido de garantir que os dados pelos quais são responsáveis pelo tratamento, são tratados na devida conformidade, uma vez que o tipo de dados tratados pelos hospitais são particularmente sensíveis e passíveis de colocar a reserva da intimidade da vida privada[5] dos cidadãos em perigo, dada a sua especial sensibilidade.

[5]A este propósito, GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada, Volume I*, 4.ª ed., Coimbra, 2007, "*os dados de saúde integram a categoria de dados relativos à vida privada, tais como as informações referentes à origem étnica, à vida familiar, à vida sexual, condenações em processo criminal, situação patrimonial e financeira*".

PARTE I – ENQUADRAMENTO

Capítulo I - Contextualização da problemática da proteção de dados perante o funcionamento dos Hospitais E.P.E.

Como teremos oportunidade de aferir ao longo do presente estudo, a proteção de dados nos hospitais do nosso país, em particular nos hospitais E.P.E., possui um especial relevo, dada a complexidade de relações existentes dentro destas instituições, aliada ao tipo de dados pessoais tratados e aos tipos de tratamentos de dados que são efetuados no âmbito das prestações de cuidados de saúde.

Bem assim, considero importante referir que, dada a dimensão das estruturas hospitalares E.P.E. em Portugal, e tendo em conta os tratamentos de dados efetuados por estas instituições, a proteção dos dados por estas tratados terá que estar necessariamente no centro das preocupações das administrações hospitalares e de todos os profissionais com responsabilidade de decisão sobre as formas de tratamento de dados, e até mesmo junto daqueles profissionais que diariamente e no desempenho das suas funções, tratam dados relativos à saúde.

No nosso país, a preocupação relativa à proteção de dados pessoais e a cultura da população em geral, no que diz respeito às matérias de privacidade é, a meu ver, menor em relação a outros países europeus. Veja-se como exemplo de país onde a cultura relativa à privacidade e à proteção de dados é mais elevada, nomeadamente a Alemanha, país onde a figura do Encarregado de Proteção de Dados existe já há mais de 8 anos, existindo inclusivamente seguros profissionais para o desempenho daquela função.

Em Portugal as preocupações relativas à proteção de dados pessoais passaram a estar em maior evidência, com a entrada em vigor do RGPD em 24 de maio de 2016, pelo que durante o período de *vacatio legis* de dois anos[6] até ao passado dia 25 de

[6] CALVÃO, Filipa, Presidente da CNPD (NEGÓCIOS, 29.01.2018): "*As empresas e o Estado tinham obrigação de preparar o regulamento desde 2016… Independentemente do valor das coimas, eu gostaria de ter visto estas preocupações, que agora existem, nos últimos anos*"

maio de 2018[7], muitas interpretações e preocupações surgiram, numa sociedade portuguesa ainda pouco experiente, em matéria de proteção de dados pessoais.

Não obstante, a grande maioria dos princípios e dos direitos dos titulares dos dados pessoais previstos no RGPD já se encontravam presentes na Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24/10/95, bem como na Lei n.º67/98 de 26 de outubro, pese embora as preocupações com a proteção de dados não tenham chegado ao nível que de momento se verifica, preocupações essas motivadas em grande parte pelas avultadas coimas, que nos casos mais graves podem ascender aos 20 milhões de euros ou a 4% da faturação anual das empresas, consoante o valor que seja mais elevado.

Voltando à realidade hospitalar, estamos cientes de que existe ainda um largo caminho a percorrer, uma vez que a abordagem a realizar à proteção de dados pessoais estará necessariamente ligada à melhoria de procedimentos internos, com o objetivo de regular as condutas e os comportamentos dos profissionais de saúde e auxiliares dessa atividade[8].

A título de exemplo, cito a conclusão do estudo de diagnóstico aos Arquivos Clínicos recentemente elaborado pela Secretaria-Geral do Ministério da Saúde, no âmbito das suas atribuições e competências[9], estudo esse realizado com base em inquéritos em que participaram Diretores Clínicos, Responsáveis do Acesso à Informação e

[7] O Regulamento Geral de Proteção de Dados teve aplicação direta em todos os Estados-Membros da União Europeia, desde o passado dia 25 de maio de 2018.

[8] Auxiliares da atividade de um Hospital, nomeadamente os serviços de apoio administrativo e serviços de apoio à administração.

[9] O diagnóstico aos Arquivos Clínicos elaborado pela Secretaria-Geral do Ministério da Saúde foi constituído por três questionários aos Responsáveis do Acesso à Informação, aos Diretores Clínicos e aos Responsáveis do Arquivo Clínico. "*No relatório, que agora se apresenta à comunidade, pretende-se identificar áreas de melhoria e prioridades de intervenção, compreender qual o impacto dos sistemas de informação na avaliação da informação clínica, analisar a qualidade dos recursos disponíveis e proceder ao levantamento da utilização e reutilização dos registos clínicos.*
Este documento estratégico reflete ainda o contexto atual e aponta caminhos futuros, que se espera virem ao encontro das reais necessidades dos profissionais de Saúde e do próprio Utente, num trabalho colaborativo e de sinergias com todos os serviços e organismos do Ministério da Saúde." O relatório está disponível para consulta no seguinte link: https://www.sns.gov.pt/wp-content/uploads/2018/06/RELATORIO_ARQUIVO_CLINICO.pdf

Responsáveis do Arquivo Clínico, e atendendo às respostas dos Responsáveis do Acesso à Informação, verificou-se que 47% dos inquiridos pertencentes a centros hospitalares refere não ter tido formação no RGPD, e 53% dos inquiridos pertencentes a hospitais refere não ter tido formação no RGPD. Na globalidade, considerando hospitais, centros hospitalares, agrupamentos de centros de saúde e unidades locais de saúde, a perspetiva é agravada, tendo em conta que apenas 35% dos inquiridos confirmaram que a Instituição lhes proporcionou formação sobre o RGPD, enquanto 65% afirmaram que não tiveram formação[10], o que revela que sabendo a especial sensibilidade dos dados tratados pelos hospitais, mesmo os profissionais com responsabilidades avultadas no tratamento de dados pessoais, não obtiveram formação adequada sobre o novo RGPD, com as consequências que o desconhecimento daquele diploma pode trazer para estas instituições de saúde, bem como para os titulares dos dados.

Apesar do supra referido, também a realidade ao nível dos sistemas da informação deve ser pensada e repensada, tendo em conta a constante digitalização e informatização da informação clínica, com as necessárias transferências e processamentos de dados pessoais em saúde, que levam a que os dados pessoais relativos à saúde sejam armazenamentos em bases de dados digitais e que muitas vezes circulem através de dispositivos de armazenamento digital ou pela internet.

Neste âmbito e a título meramente exemplificativo da vulnerabilidade da informação clínica dos utentes, menciono o ataque informático que ocorreu em finais do ano de 2016 ao Hospital Garcia de Orta "*O ciberataque aconteceu no final de 2016 e foi comunicado pela unidade às entidades competentes... Foi atingido o sistema onde são guardados imagens obtidas em exames médicos como radiografias ou TAC mas a unidade garante que não foram roubados registos de doentes…. este é o maior ataque informático registado num hospital do Serviço Nacional de Saúde alguma vez conhecido, isto numa altura em que a Comissão Nacional de Proteção de*

[10] É de notar que estes resultados são ainda mais preocupantes, se tivermos em conta que os profissionais inquiridos são profissionais que lidam especificamente com proteção de dados e que decidem muitas vezes sobre as formas de tratamentos de dados de saúde.

Dados tem reforçado os alertas para que sejam adotados sistemas mais robustos e com informação encriptada para proteger a privacidade dos cidadãos.[11]*".*

Teremos portanto a oportunidade de perceber ao longo do nosso estudo, as maiores implicações ao nível da proteção de dados nos hospitais e centros hospitalares E.P.E. e de que forma estas entidades podem proteger devidamente os dados pessoais dos seus utentes por um lado, e salvaguardarem a sua posição perante os utentes e as entidades fiscalizadoras, evitando uma das problemáticas que será central no nosso estudo, nomeadamente a responsabilidade civil extracontratual por violação de dados pessoais.

[11] Piratas informáticos atacam hospital Garcia de Orta:
https://sol.sapo.pt/artigo/549734/piratas-informaticos-atacam-hospital-garcia-de-orta-

Capítulo II - Sistema de Saúde e Serviço Nacional de Saúde

A Lei de Bases da Saúde, aprovada pela Lei n.º 48/90, de 24 agosto, atualizada pela Lei n.º 27/2002, de 08 de novembro, estabelece os princípios pelos quais o Estado deve reger a sua atuação, no sentido de proteger o direito dos cidadãos à proteção da saúde.[12]

A base IV, cuja epígrafe é *Sistema de Saúde e Outras Entidades*, prevê no seu n.º1, que "*O sistema de saúde visa a efetivação do direito à proteção da saúde*.". Ainda de acordo com o n.º2 da base IV, "*Para efetivação do direito à proteção da saúde, o Estado atua através de serviços próprios, celebra acordos com entidades privadas para a prestação de cuidados e apoia e fiscaliza a restante atividade privada na área da saúde*". Estabelece ainda o n.º3 da base IV, que "*Os cidadãos e as entidades públicas e privadas devem colaborar na criação de condições que permitam o exercício do direito à proteção da saúde e a adoção de estilos de vida saudáveis"*.

No Capítulo II daquele diploma, nomeadamente o que versa acerca das entidades prestadoras de cuidados de saúde em geral, estabelece o n.º1 da base XII que "*O sistema de saúde é constituído pelo Serviço Nacional de Saúde e por todas as entidades públicas*[13] *que desenvolvam atividades de promoção, prevenção e tratamento na área da saúde, bem como por todas as entidades privadas e por todos os profissionais livres que acordem com a primeira a prestação de todas ou de algumas daquelas atividades*".

Por outro lado, estatui o n.º 2 da base XII que "*O Serviço Nacional de Saúde abrange todas as instituições e serviços oficiais prestadores de cuidados de saúde dependentes do Ministério da Saúde e dispõe de estatuto próprio*"[14].

Tal separação de definições entre Sistema de Saúde e Serviço Nacional de Saúde, esclarece que o Serviço Nacional de Saúde está incluído no Sistema de Saúde, apesar deste último não se esgotar nas entidades públicas de prestação de cuidados de

[12] Como o objeto da minha dissertação está enquadrado na responsabilidade civil das administrações dos hospitais e centros hospitalares E.P.E. por violação em matéria de proteção de dados pessoais relativos à saúde, deixarei fora da discussão a referência aos organismos privados de prestação de cuidados de saúde.
[13] Sublinhado nosso.
[14] Sublinhado nosso.

saúde, englobando ainda todas as entidades privadas e os profissionais livres que exercem a atividade de medicina.

Fazem portanto parte do Serviço Nacional de Saúde, de acordo com o estipulado no n.º2 do artigo 7º da Lei Orgânica do Ministério da Saúde (LOMS), aprovada pelo Decreto-Lei n.º 124/2011, de 29 de dezembro **"***todos os serviços e entidades públicas prestadoras de cuidados de saúde, designadamente os agrupamentos de centros de saúde, os estabelecimentos hospitalares, independentemente da sua designação, e as unidades locais de saúde*", nos quais se devem incluir todos os Agrupamentos de Centros de Saúde (ACES), os estabelecimentos hospitalares (Hospitais e Centros Hospitalares), bem como as Unidades Locais de Saúde (ULS).

De acordo com o preceituado no n.º1 do artigo 7º da LOMS, "*O membro do Governo responsável pela área da saúde exerce poderes de superintendência e tutela, nos termos da lei, sobre todos os serviços e estabelecimentos do SNS, independentemente da respetiva natureza jurídica*".

Capítulo III - A relação jurídica administrativa de prestação de cuidados de saúde

No âmbito deste estudo, considero pertinente que se realize uma breve abordagem de enquadramento acerca da relação jurídica administrativa da prestação de cuidados de saúde, nomeadamente aquela relativa às prestações de cuidados de saúde dentro do Serviço Nacional de Saúde, onde se enquadram naturalmente todos os hospitais e centro hospitalares, E.P.E., como já tivemos oportunidade de aferir.

Esta abordagem tem importância no âmbito do regime de responsabilidade civil extracontratual do Estado e demais entidades públicas, porquanto a relação existente no âmbito da prestação de cuidados de saúde se trata de uma relação jurídica administrativa, não se considerando a existência de uma relação contratual entre a instituição prestadora de cuidados de saúde e o utente. Neste sentido Maria João Estorninho e Tiago Macieirinha "*ao contrário do que sucede no Direito Privado, esta relação jurídica não parece ter a sua fonte no contrato, ou seja, no acordo de vontades das partes, mas antes surge como consequência do acesso dos cidadãos… ao serviço público de saúde, determinado por uma permissão normativa de origem legal ou mesmo constitucional*"[15].

A este propósito, refere o professor Sérvulo Correia[16] que "*Um ponto comum às relações jurídicas administrativas de prestação de cuidados de saúde é o seu carácter não contratual.*", defendendo que o ato que cria a relação de utilização de um serviço que pertence ao Serviço Nacional de Saúde não é bilateral, por não se materializar num acordo de vontades. Refere ainda o professor Sérvulo Correia que "*O utente, ou alguém por ele, requer uma consulta, a qual deverá ser-lhe concedida de acordo com o princípio da máxima acessibilidade possível, traduzido em atendimento no próprio dia e marcação de consulta para hora determinada. À formulação da pretensão corresponderá, portanto, uma decisão de concessão imediata de consulta ou de marcação de consulta. Eventualmente, em articulação com uma consulta, poderá ser*

[15]ESTORNINHO, Maria João e MACIEIRINHA, Tiago – *Direito da Saúde* – Lisboa, Universidade Católica Editora, 2014;
[16] SÉRVULO CORREIA, José Manuel – As relações jurídicas administrativas de prestação de cuidados de saúde, em: https://www.icjp.pt/sites/default/files/media/616-923.pdf

determinado um internamento em hospital ou em unidade de internamento do próprio centro de saúde."

Deste modo, considero que a relação jurídico administrativa de prestação de cuidados de saúde no âmbito do Serviço Nacional de Saúde apresenta uma fonte legislativa e uma fonte regulamentar, na medida em que é necessário atender às diferenças ao nível das instituições prestadoras de cuidados de saúde com base em imposições legais, em paralelismo com as disposições regulamentares ao nível dos regulamentos internos das instituições.

Defende ainda o professor Sérvulo Correia[17], que "*São deste modo praticados actos administrativos ampliativos, sob solicitação do particular ou antecedidos do seu consentimento. O valor das vontades manifestadas pelo particular e pela Administração de Saúde e o conteúdo das faculdades e poderes exercidos não se equiparam.",* na medida em que quando o utente aceita a prestação de cuidados de saúde, ou recusa essa mesma prestação "*cria um pressuposto de uma decisão positiva ou negativa*", apesar da prestação de cuidados de saúde em si, estar exclusivamente dependente da vontade da instituição de saúde. Defende o professor Sérvulo Correia que "*no plano estrutural, a marcação de consulta ou a decisão de internamento são manifestações unilaterais da vontade da Administração, constitutivas de uma relação específica de prestação de serviços (cuidados) de saúde, que se articulam com manifestações de vontade do particular",* enquanto que a manifestação de vontade do utente em aceitar ou não a prestação de cuidados de saúde, representa um requisito de "*validade ou de eficácia da decisão administrativa, consoante esta dependa legalmente de um pedido prévio ou do consentimento do utente, quando este deva ou possa ser posterior ao acto ainda que anterior à respectiva execução material*". Ainda assim, acompanhado a posição de Maria João Estorninho e Tiago Macieirinha, concordo que a relação existente entre a instituição prestadora de cuidados de saúde e o utente, não se trata de uma relação especial de poder, na medida em que se forma uma verdadeira relação jurídica "*cujo conteúdo mais ou menos determinado, não autoriza a recondução do utente à situação de sujeição às*

[17] SÉRVULO CORREIA, José Manuel – As relações jurídicas administrativas de prestação de cuidados de saúde, em: https://www.icjp.pt/sites/default/files/media/616-923.pdf

regras do serviço, mas antes à condição de titular de verdadeiros e próprios direitos de crédito, cujo cumprimento pode exigir.[18]"

[18] ESTORNINHO, Maria João e MACIEIRINHA, Tiago – *Direito da Saúde* – Lisboa, Universidade Católica Editora, 2014;

Capítulo IV – Constituição da República Portuguesa: Direito à Saúde e Direito à reserva da intimidade da vida privada

A Constituição da República Portuguesa dedica à área da saúde um artigo denso e complexo, estabelecendo o direito a todos os cidadãos quanto à proteção da saúde, bem como quanto ao dever de a defender e de a promover. A Constituição da República Portuguesa estatui, portanto, um direito fundamental à proteção da saúde, inserido no capítulo que enuncia os Direitos e os Deveres Sociais, nomeadamente no n.º1 do artigo 64º, *"Todos têm direito à proteção da saúde e o dever de a defender e promover".*

Encontra-se ainda estatuído na alínea a) do nº2 do artigo 64º da CRP, que o direito à proteção da saúde é realizado "*através de um serviço nacional de saúde universal e geral e, tendo em conta as condições económicas e sociais dos cidadãos, tendencialmente gratuito*"[19].

A CRP estabelece também no artigo 26º, no capítulo referente aos direitos, liberdades e garantias pessoais o seguinte: "*A todos são reconhecidos os direitos à identidade pessoal… ao bom nome e à reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação*", garantido aqui a CRP que o direito à privacidade e à reserva da intimidade da vida privada são efetivamente um direito fundamental. Sobre esta questão, o Ac. nº 128/92, do TC de 1 de Abril de 1992[20] pronunciou-se sobre a reserva da intimidade da vida privada que "*Trata-se do direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias. É a privacy do direito anglo-saxónico"*.

No âmbito da prestação de cuidados de saúde e acompanhando o entendimento de Maria João Estorninho e Tiago Macieirinha sobre o segredo médico "*a imposição do segredo cumpre… função especial… que se prende com a tutela da reserva da intimidade da vida privada do paciente… Nestes termos, a imposição do segredo*

[19] Sublinhado nosso.
[20] Acórdão nº 128/92, de 1 de Abril de 1992 do Tribunal Constitucional

encontra o seu fundamento essencial na reserva da vida privada do paciente, a qual, como é sabido, merce tutela constitucional"[21].

Mais, a CRP dedica um artigo à matéria da proteção de dados pessoais, nomeadamente o seu artigo 35º. Assim, encontra-se estipulado no artigo 35º que "*A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente*.". Encontra-se ainda estatuído que "*É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei", estando ainda previsto que "os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista*…" para os dados informatizados, nos termos do artigo 35º da CRP.

Também a Convenção Europeia dos Direitos do Homem[22] dispõe no artigo 8º n.º1 que "*Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*" e no n.º2 que "*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 infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros*".

Deste modo, reiteramos que a proteção de dados em Portugal não é um assunto desconhecido[23], estando inclusivamente previsto na própria lei fundamental, reconhecendo o legislador português a importância da proteção dos dados dos titulares.

[21]ESTORNINHO, Maria João e MACIEIRINHA, Tiago – *Direito da Saúde* – Lisboa, Universidade Católica Editora, 2014;
[22] Convenção Europeia dos Direitos do Homem, adotada pelo Conselho da Europa, em 4 de novembro de 1950.
[23] O direito à reserva da intimidade da vida privada foi consagrado pela primeira vez em Portugal, no Código Civil de 1966.

Capítulo V - Hospitais E.P.E. e Centros Hospitalares E.P.E.

Para melhor percebermos o funcionamento dos hospitais e centros hospitalares E.P.E., será necessário efetuar uma análise à sua estrutura interna, bem como às competências de cada órgão e Serviço estatutariamente previstos. Como teremos oportunidade de analisar, não se encontra previsto no Decreto-Lei n.º 18/2017 de 10 de fevereiro[24], nem nos estatutos a ele anexos, qualquer disposição especial relativa à proteção de dados pessoais, nem a previsão de existência de serviço, núcleo ou comissão que se preocupe em especial com a proteção de dados pessoais. Esta falta de disposição será, no meu entendimento, uma lacuna que reflete também o nível de desadequação e de preocupação da tutela, nomeadamente do ministério da saúde, no que as matérias relativas à proteção de dados pessoais diz respeito.

Os hospitais E.P.E. e os centros Hospitalares E.P.E. são, quanto à sua natureza, e de acordo com o preceituado no n.º1 do artigo 18º do Decreto-Lei n.º18/2017 de 10 de fevereiro, pessoas coletivas de direito público de natureza empresarial dotadas de autonomia administrativa, financeira e patrimonial, nos termos do regime jurídico do sector público empresarial. Tal previsão está igualmente contemplada no n.º 1 do artigo 1º dos Estatutos dos Hospitais, Centros Hospitalares e Institutos Portugueses de Oncologia, E.P.E., anexo II[25] ao Decreto-Lei n.º 18/2017 de 10 de fevereiro.

O objeto dos hospitais e centros hospitalares E.P.E. é, segundo o definido no artigo 2º dos já referidos estatutos, "*a prestação de cuidados de saúde a todos os cidadãos em geral, designadamente, aos utentes do Serviço Nacional de Saúde, às entidades externas que com ele contratualizem a prestação de cuidados de saúde e aos cidadãos estrangeiros não residentes, no âmbito da legislação nacional e internacional em vigor*."[26]

[24] DL n.º 18/2017, de 10 de Fevereiro – Regime Jurídico e Estatutos aplicáveis às unidades de saúde do Serviço Nacional de Saúde.
[25] Anexo II ao DL n.º 18/2017, de 10 de Fevereiro, que contem os Estatutos dos Hospitais, Centros Hospitalares e Institutos Portugueses de Oncologia, E.P.E.
[26] Como veremos em seguida, a prossecução deste objeto não será possível sem o tratamento de dados relativos à saúde dos utentes. É também esse o entendimento do Grupo de Trabalho do Artigo 29º, quando aprecia a atividade de um hospital, para efeitos de

Os hospitais e centros hospitalares E.P.E. têm ainda como objeto, o desenvolvimento de atividades de investigação, formação e ensino, sendo a sua participação na formação de profissionais de saúde dependente da respetiva capacidade formativa, podendo ser objeto de contratos-programa, em que se definam as respetivas formas de financiamento.

Os hospitais e centros hospitalares E.P.E. possuem um vasto leque de regulamentos administrativos de índole interna, desde o Regulamento Interno da própria instituição, até aos diversos regulamentos de Serviços de natureza assistencial e de apoio à administração, que fixam diretrizes mais específicas, consoante as necessidades atuais da população da área de abrangência da instituição, mas também acompanhando as atualizações legislativas e as orientações do próprio Ministério da Saúde[27].

Assim, importa explanar, para um melhor enquadramento das questões a tratar, que os hospitais e centros hospitalares E.P.E. se encontram na tutela do Ministério da Saúde, sendo que, de acordo com o plasmado no artigo 6º do Decreto-Lei n.º 18/2017 de 10 de fevereiro, o membro do Governo responsável pela área da saúde exerce sobre estes, "*poderes de definição das normas e critérios de atuação hospitalar, definição das diretrizes a que devem obedecer os planos e programas de ação, bem como a avaliação da qualidade dos resultados obtidos nos cuidados prestados à população, acesso a todas as informações julgadas necessárias ao acompanhamento da atividade, determinação da restrição da autonomia gestionária na situação de desequilíbrio económico-financeiro e determinação de auditorias e inspeções ao seu funcionamento, nos termos da legislação aplicável*."

aferição do conceito de atividade principal "*Por exemplo, a atividade principal de um hospital é a prestação de cuidados de saúde. Contudo, um hospital não poderia prestar cuidados de saúde de forma segura e eficaz sem proceder ao tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes. Assim, o tratamento destes dados deve ser considerado uma das atividades principais de qualquer hospital*…", em Orientações sobre os encarregados da proteção de dados (EPD) – Grupo de Trabalho do Artigo 29º

[27] No capítulo II da Parte III do presente estudo, teremos oportunidade de propor a adoção de um Regulamento Interno Relativo aos dados pessoais para as instituições de saúde, encontrando-se ainda em anexo (anexo 1) ao presente estudo um exemplo de regulamento interno que poderá ser adotado.

Relativamente à superintendência destas instituições, "*cabe ao membro do Governo responsável pela área da saúde, definir os objetivos e as estratégias das E.P.E., integradas no SNS, emitir orientações, recomendações e diretivas específicas para prossecução da atividade operacional das E.P.E. integradas no SNS, bem como definir normas de organização e de atuação hospitalar, não obstante estes poderes poderem ser delegados nos conselhos diretivos da Administração Central do Sistema de Saúde, I.P. (ACSS, I.P.) e da Administração Regional de Saúde territorialmente competente*".[28]

Os Hospitais e Centros Hospitalares E.P.E. estão sujeitos à tutela setorial do Ministério da Saúde e à tutela financeira do Ministério das Finanças.

Nestes termos, "*compete ao membro do Governo responsável pela área da saúde, exigir todas as informações julgadas necessárias ao acompanhamento da atividade das E.P.E., integradas no SNS, sem prejuízo da prestação de outras legalmente exigíveis, determinar auditorias e inspeções ao funcionamento das E.P.E, integradas no SNS, de acordo com a legislação aplicável, homologar os regulamentos internos das E.P.E. integradas no SNS e praticar outros atos que, nos termos da lei, careçam de autorização prévia ou aprovação tutelar*."[29]

São órgãos dos Hospitais e Centros Hospitalares E.P.E. o Conselho de Administração, o Conselho Fiscal, o Revisor Oficial de Contas ou uma Sociedade de Revisores Oficiais de Contas, caso se encontrem abrangidas pelo regime constante da Lei n.º 148/2015, de 9 de Setembro, ou o fiscal único e o conselho consultivo[30], sendo estes últimos órgãos de fiscalização.

Em termos de organização interna, as E.P.E. integradas no SNS organizam-se de acordo com as normas e critérios genéricos definidos pela tutela em função das suas atribuições e áreas de atuação específicas, devendo os respetivos regulamentos internos prever a estrutura orgânica com base em serviços agregados em departamentos e englobando unidades funcionais, bem como estruturas orgânicas de gestão intermédia.

[28] Artigo 19º, n.º1 e 2 do DL n.º 18/2017 de 10 de fevereiro.
[29] Artigo 20º n.º 1 do DL n.º 18/2017 de 10 de fevereiro.
[30] Artigo 5º do Anexo II do DL n.º 18/2017 de 10 de fevereiro.

Neste âmbito, cumpre ainda referir o estatuído na Portaria n.º 147/2016 de 19 de maio, que estabelece o processo de classificação dos hospitais, centros hospitalares e unidades locais de saúde do Serviço Nacional de Saúde, independentemente da sua natureza jurídica, tendo como princípio a definição das Redes de Referenciação Hospitalar. Com efeito, prevê esta portaria no n.º1 do artigo 3º que "*os hospitais, centros hospitalares e unidades locais de saúde classificam-se em grupos, de acordo com as respetivas especialidades desenvolvidas, a população abrangida, a capacidade de formação, a diferenciação dos recursos humanos, o modelo de financiamento, a classificação dos seus serviços de urgência e a complexidade da produção hospitalar.*"

1. Conselho de Administração

O conselho de administração é composto pelo "*presidente e um máximo de quatro vogais, que exercem funções executivas, em função da dimensão e complexidade do Hospital E.P.E., incluindo um diretor clínico, um enfermeiro-diretor e um vogal proposto pelo membro do Governo responsável pela área das finanças"*[31]. Os membros do conselho de administração são designados de entre individualidades que reúnam os requisitos previstos no Estatuto do Gestor Público[32] e possuam preferencialmente "*evidência curricular de formação específica em gestão em saúde e experiência profissional adequada, sendo o diretor clínico um médico[33], e o enfermeiro-diretor um enfermeiro"*[34]. O requisito de inclusão de dois profissionais da área dos serviços assistenciais, como pertencentes obrigatoriamente ao conselho de administração, faz crer que o legislador pretendeu deliberadamente incluir no órgão máximo de gestão destas instituições, indivíduos com experiência profissional de natureza assistencial, afastando uma lógica de gestão puramente economicista e incluindo no processo decisório indivíduos com experiência prática e conhecedores do "terreno"[35]. O mandato dos membros do Conselho de Administração tem a

[31] Artigo 6º, n.º1 do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[32] Estatuto do Gestor Público - DL n.º 71/2007, de 27 de Março
[33] Artigo 6º, n.º2 do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[34] Artigo 6º, n.º2 do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[35] No âmbito da proteção de dados pessoais relativos à saúde, os papéis do Diretor Clínico e do Enfermeiro-Diretor são preponderantes, na medida em que estes profissionais lidam, à partida, desde o início da sua formação base com dados sensíveis relativos à saúde, o que

"*duração de três anos renovável e é renovável uma única vez, permanecendo aqueles no exercício das suas funções até à designação dos novos titulares, sem prejuízo da que possa haver"*[36].

Ao Conselho de Administração compete "*garantir o cumprimento dos objetivos básicos, bem como o exercício de todos os poderes de gestão que não estejam reservados a outros órgãos"*[37]. Compete ainda, e especialmente, ao Conselho de Administração, as seguintes tarefas, definidas nas alíneas infra, plasmadas no n.º1 do artigo 7º do anexo II do DL n.º 18/2017 de 10 de fevereiro:

a) Propor os planos de atividades anuais e plurianuais e respetivos orçamentos, bem como os demais instrumentos de gestão previsional legalmente previstos, e assegurar a respetiva execução;

b) Celebrar contratos-programa externos e internos;

c) Definir as linhas de orientação a que devem obedecer a organização e o funcionamento do hospital E. P. E., nas áreas clínicas e não clínicas, de novos serviços, sua extinção ou modificação;

d) Definir as políticas referentes a recursos humanos, incluindo as remunerações dos trabalhadores e dos titulares dos cargos de direção e chefia;

e) Autorizar a realização de trabalho extraordinário e de prevenção dos trabalhadores do hospital E. P. E., independentemente do seu estatuto, bem como autorizar o respetivo pagamento;

f) Designar o pessoal para cargos de direção e chefia;

g) Aprovar o regulamento disciplinar do pessoal e as condições de prestação e disciplina do trabalho;

h) Apresentar os documentos de prestação de contas, nos termos definidos na lei;

---

poderá resultar numa maior sensibilidade para as questões da proteção de dados de saúde. Para esta questão releva ainda o facto de nalguns hospitais, as funções de Responsável do Acesso à Informação serem desempenhadas pelo Diretor-Clínico.

[36] Artigo 6º, n.º 4 do Anexo II do DL n.º 18/2017 de 10 de fevereiro

[37] Artigo 7º, n.º1 do Anexo II do DL n.º 18/2017 de 10 de fevereiro

i) Aprovar e submeter a homologação do membro do Governo responsável pela área da saúde o regulamento interno e fazer cumprir as disposições legais e regulamentares aplicáveis;

j) Decidir sobre a realização de ensaios clínicos e terapêuticos, ouvida a comissão de ética, sem prejuízo do cumprimento das disposições aplicáveis;

k) Acompanhar e avaliar sistematicamente a atividade desenvolvida pelo hospital E. P. E., designadamente responsabilizando os diferentes setores pela utilização dos meios postos à sua disposição e pelos resultados atingidos, nomeadamente em termos da qualidade dos serviços prestados;

l) Tomar conhecimento e determinar as medidas adequadas, se for caso disso, sobre as queixas e reclamações apresentadas pelos utentes;

m) Decidir sobre a admissão e gestão do pessoal;

n) Autorizar a aplicação de todas as modalidades de regimes de trabalho legalmente admissíveis;

o) Exercer a competência em matéria disciplinar prevista na lei, independentemente da relação jurídica de emprego;

p) Acompanhar a execução do orçamento, aplicando as medidas destinadas a corrigir os desvios em relação às previsões realizadas;

q) Assegurar a regularidade da cobrança das dívidas e autorizar a realização e o pagamento da despesa do hospital E. P. E.;

r) Tomar as providências necessárias à conservação do património afeto ao desenvolvimento da sua atividade e autorizar as despesas inerentes, previstas no plano de investimentos.

O conselho de administração detém ainda as "*competências legalmente atribuídas aos titulares dos cargos de direção superior do 1º grau da administração central do Estado, relativamente aos trabalhadores da Administração Pública"*. O conselho de administração "*poderá ainda delegar as suas competências nos seus membros, ou*

demais pessoal de direção e chefia, incluindo os diretores dos Centros de Responsabilidade Integrada, com exceção das previstas nas alíneas a) a j) do n.º1, definindo em ata os limites e condições do seu exercício"[38].

Julgamos ainda pertinente referir, que o conselho de administração se obriga pela assinatura, com indicação de qualidade, de dois membros do conselho de administração ou de quem esteja legitimado para o efeito, nos termos de eventual delegação de competências[39].

2. Presidente do conselho de administração

Compete ao conselho de administração dos hospitais e centros hospitalares E.P.E., "*coordenar a atividade dos conselho de administração e dirigir as respetivas reuniões, garantir a correta execução das deliberações do conselho de administração, submeter a aprovação ou a autorização dos membros do Governo competentes todos os atos que delas careçam, representar o Hospital E.P.E., em juízo e fora dele e em convenção arbitral, podendo designar mandatários para o efeito constituídos e exercer as competências que lhe sejam delegadas"*. O presidente do conselho de administração é substituído nas suas ausências e impedimentos pelo vogal por si designado[40].

3. Diretor Clínico

O diretor clínico dirige a produção clínica do Hospital E.P.E., que compreende a coordenação da assistência prestada aos doentes e a qualidade, correção e prontidão dos cuidados de saúde prestados.

Designadamente, compete ao diretor clínico[41]:

[38] Artigo 7º, n.ºs 2 e 3 do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[39] Artigo 12º do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro
[40] Artigo 8º, n.ºs 1 e 2 do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[41] Artigo n.º 9 do Anexo II do DL n.º 18/2017 de 10 de fevereiro.

a) *Coordenar a elaboração dos planos de ação apresentados pelos vários serviços e departamentos de ação médica a integrar no plano de ação global do hospital;*
b) *Assegurar uma integração adequada da atividade médica dos departamentos e serviços, designadamente através de uma utilização não compartimentada da capacidade instalada;*
c) *Propor medidas necessárias à melhoria das estruturas organizativas, funcionais e físicas dos serviços de ação médica, dentro de parâmetros de eficiência e eficácia reconhecidos, que produzam os melhores resultados face às tecnologias disponíveis;*
d) *Aprovar as orientações clínicas relativas à prescrição de medicamentos e meios complementares de diagnóstico e terapêutica, bem como os protocolos clínicos adequados às patologias mais frequentes, respondendo perante o conselho de administração pela sua adequação em termos de qualidade e de custo-benefício;*
e) *Propor ao conselho de administração a realização, sempre que necessário, da avaliação externa do cumprimento das orientações clínicas e protocolos mencionados, em colaboração com a Ordem dos Médicos e instituições de ensino médico e sociedades científicas;*
f) *Desenvolver a implementação de instrumentos de garantia de qualidade técnica dos cuidados de saúde, em especial no que diz respeito aos indicadores de desempenho assistencial e segurança dos doentes, reportando e propondo correção em caso de desvios;*
g) *Decidir sobre conflitos de natureza técnica entre serviços de ação médica;*
h) *Decidir as dúvidas que lhe sejam presentes sobre deontologia médica, desde que não seja possível o recurso, em tempo útil, à comissão de ética;*
i) *Participar na gestão do pessoal médico, designadamente nos processos de admissão e mobilidade interna, ouvidos os respetivos diretores de serviço;*
j) *Velar pela constante atualização do pessoal médico e acompanhar e avaliar sistematicamente outros aspetos relacionados com o exercício da medicina e com a formação dos médicos.*

4. Enfermeiro-diretor

Ao enfermeiro-diretor compete a coordenação técnica da atividade de enfermagem do Hospital E.P.E., velando pela sua qualidade.

Compete designadamente ao enfermeiro-diretor[42]:

a) *Coordenar a elaboração dos planos de ação de enfermagem apresentados pelos vários serviços a integrar no plano de ação global do hospital E. P. E.;*
b) *Colaborar com o diretor clínico na compatibilização dos planos de ação dos diferentes serviços de ação médica;*
c) *Contribuir para a definição das políticas ou diretivas de formação e investigação em enfermagem;*
d) *Definir padrões de cuidados de enfermagem e indicadores de avaliação dos cuidados de enfermagem prestados;*
e) *Elaborar propostas referentes à gestão do pessoal de enfermagem, designadamente participar no processo de admissão e de mobilidade dos enfermeiros;*
f) *Promover e acompanhar o processo de avaliação do pessoal de enfermagem;*
g) *Propor a criação de um sistema efetivo de classificação de utentes que permita determinar necessidades em cuidados de enfermagem e zelar pela sua manutenção, elaborar estudos para determinação de custos e benefícios no âmbito dos cuidados de enfermagem;*
h) *Acompanhar e avaliar sistematicamente outros aspetos relacionados com o exercício da atividade de enfermagem e com a formação dos enfermeiros.*

5. Estatuto dos Membros

Aos membros do conselho de administração aplica-se o Estatuto do Gestor Público[43], sem prejuízo do estatuído no Decreto-Lei n.º 18/2017, de 10 de fevereiro[44].

[42] Artigo 10º do Anexo II do DL n.º 18/2017 de 10 de fevereiro
[43] Estatuto do Gestor Público - DL n.º 71/2007, de 27 de Março
[44] Artigo 13º, n.º1 do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro

6. Serviço de auditoria interna

Neste ponto, mesmo não estando tipificado como um verdadeiro órgão do Hospital E.P.E., julgamos pertinente explanar nesta dissertação as competências do serviço de auditoria interna, "*responsável pela avaliação dos processos de controlo interno e de gestão de riscos, nos domínios contabilístico, financeiro, operacional, informático e de recursos humanos, contribuindo para o seu aperfeiçoamento contínuo"*. São competências especiais do serviço de auditoria interna do Hospital E.P.E., "*fornecer ao conselho de administração análises e recomendações sobre as atividades revistas para melhoria do funcionamento dos serviços, receber as comunicações de irregularidades sobre a organização e funcionamento do Hospital E.P.E., apresentadas pelos demais órgãos estatutários, trabalhadores, colaboradores, utentes e cidadãos em geral, elaborar o plano anual de auditoria interna, elaborar anualmente um relatório sobre a atividade desenvolvida, em que se refiram os controlos efetuados, as anomalias detetadas e as medidas corretivas a adotar e elaborar o plano de gestão de riscos de corrupção e infrações conexas e os respetivos relatórios anuais de execução"*[45].

O Serviço de auditoria interna poderá ter um papel preponderante no auxílio do Encarregado de Proteção de Dados, no desempenho das suas funções, nomeadamente as funções de auditoria em matéria de proteção de dados. Assim, se bem que as funções não se confundem, cabendo ao Encarregado de Proteção de Dados a realização de auditorias internas, o Serviço de auditoria interna poderá acompanhar o EPD, prestando auxílio, nomeadamente tendo em conta o conhecimento profundo dos serviços das instituições e dos seus procedimentos internos, muitos deles também relativos ao tratamento de dados pessoais de categorias especiais.

O serviço de auditoria interno "*é dirigido por um auditor interno, que exerce as respetivas funções pelo período de três anos, renovável por iguais períodos, até ao limite máximo de três renovações consecutivas ou interpoladas e que é apoiado tecnicamente nas suas funções por um máximo de três técnicos auditores. O auditor interno é recrutado pelo conselho de administração, de entre individualidades que*

[45] Artigo 19º, n.º 2 do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro

reúnam requisitos de qualificação técnica, competências e experiência em auditoria, e inscrição no organismo nacional que regule a atividade de auditoria interna"[46].

7. Comissões de Apoio Técnico

Nos estatutos dos Hospitais e Centros Hospitalares E.P.E. estão ainda previstas a existências de comissões de apoio técnico, que estão tipificadas como órgãos de caráter consultivo que têm por função colaborar com o conselho de administração, por sua iniciativa ou a pedido daquele, nas matérias da sua competência.

Neste âmbito, em cada Hospital E.P.E., existem a comissão de ética, a comissão de qualidade e segurança do doente, o grupo de coordenação local do Programa de Prevenção e Controlo de Infeções e de Resistência aos Antimicrobianos e a comissão de farmácia e terapêutica.

Os pareceres emanados por estas comissões têm relevância, nomeadamente naquela que é a fixação ou definição de regras de conduta, que embora não tenham força de lei, o seu desrespeito ou não seguimento, pode implicar a violação das *leges artis,* com relevância no apuramento de responsabilidade por erros técnicos ou por más práticas.

No Capítulo II da parte III, teremos oportunidade de propor a criação de uma equipa afeta à implementação do RGPD, que num momento futuro e após a implementação do RGPD, poderá funcionar sobre a forma de Comissão Técnica (Comissão de Proteção de Dados), podendo ter a função de emitir orientações e recomendações ao responsável pelo tratamento sobre as formas de tratamento, sempre em estreita articulação com o EPD.

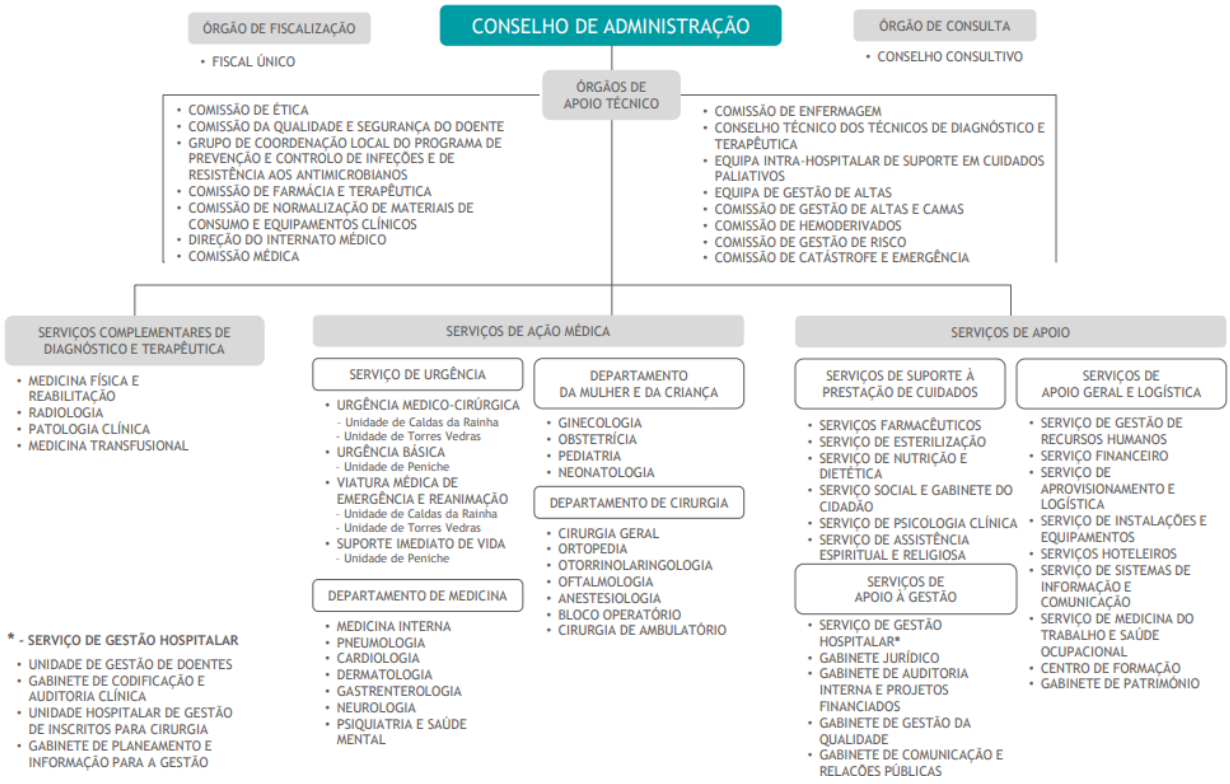
Aqui chegados, conseguimos obter um panorama geral sobre o funcionamento orgânico interno dos hospitais e centros hospitalares do nosso país, compreendendo a sua dimensão e complexidade organizacional, nomeadamente ao nível dos órgãos previstos nos estatutos e dos restantes serviços institucionais.

[46] Artigo 19º, n.º 3 e 4 do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro

Dada a sua relevância no âmbito do nosso estudo, não será de descurar a referência aos Serviços de natureza assistencial e das áreas de apoio à administração, divididos pelas várias especialidades clínicas, nos quais se incluem os profissionais da área médica, bem como da área de enfermagem, assistentes operacionais e também os profissionais assistentes técnicos, maioritariamente integrados nos Serviços de Gestão de Doentes, prestando um apoio essencial no bom desempenho dos serviços da área assistencial.

8. Organograma tipo de um Centro Hospitalar

Como exemplo de um organograma-tipo de um Hospital E.P.E., podemos referir a seguinte estrutura organizacional[47]:



[47] O organograma supra exposto é exclusivamente ilustrativo, tendo sido retirado do seguinte endereço eletrónico, disponível para consulta pública, disponibilizado pelo Centro Hospitalar do Oeste:
http://www.choeste.min-saude.pt/images/conteudos/OCHO/Organograma/Organograma_CHO_aprovado.pdf

PARTE II – PROTEÇÃO DE DADOS EM SAÚDE E NOS HOSPITAIS E.P.E.

Capítulo I - O tratamento de dados como fator essencial da prestação de cuidados de saúde

O tratamento de dados pessoais relativos à saúde de uma pessoa, está intimamente ligado à prestação de cuidados de saúde ministrada aos utentes do Serviço Nacional de Saúde, como condição acessória e necessária aquela prestação de cuidados.

A medicina nos nossos dias é praticada tendo por base o historial clínico do doente, sendo que em muitos casos, quando um doente entra numa instituição do SNS, nomeadamente nos Hospitais E.P.E, é possível rastrear todos os cuidados de saúde que lhe foram ministrados, muitas vezes desde o momento do seu nascimento. A este propósito Sérgio Deodato refere que a intervenção de saúde, que tipifica como global, implica "*um conhecimento do passado histórico de cada pessoa, que muitas vezes obriga a um conhecimento prévio familiar, naquilo a que se denomina pela «história pessoa e familiar de saúde». Ou seja, a intervenção de saúde necessita aprofundar significativamente o conhecimento sobre a pessoa e a sua família, para que possa diagnosticar e intervir de forma eficaz*"[48].

A realidade do Serviço Nacional de Saúde e dos Hospitais E.P.E. é díspar, se bem que em matéria de tratamento de dados, os Hospitais possuem os arquivos físicos, onde se encontram arquivados os processos clínicos ditos mais antigos, sendo que muitos deles se encontram ainda em fase de digitalização desses mesmos processos para bases de dados informáticas.

Ora, conhecendo a realidade da saúde e sabendo que a transformação digital no SNS se tem dado a uma velocidade bastante relevante, é impossível afastar que o risco inerente ao tratamento[49] de dados no seu todo (recolha, armazenamento, consulta,

[48] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;
[49] Artigo 4º, n.º2 - Definição de tratamento de dados

apagamento, etc.), acarreta um elevado risco, quer para os titulares quer para os responsáveis pelo tratamento e mesmo para os subcontratantes.

Nos hospitais são vários os programas informáticos e aplicações que contêm bases de dados e que tratam dados de doentes, sendo diversos os profissionais daquelas instituições que consultam informação no normal exercício da sua função de prestadores de cuidados de saúde ou de auxiliares daquela função. A este propósito, refere Sérgio Deodato que a informação recolhida pelos profissionais de saúde "*não é apenas do conhecimento de um profissional de saúde, mas de uma equipa multidisciplinar. A assistência em saúde assume hoje um contexto particularmente complexo, onde os problemas de saúde-doença das pessoas exigem uma resposta pluriprofissional. E faz-se sobretudo no âmbito de organizações de saúde, como os hospitais ou os centros de saúde, onde estas equipas registam os diversos dados de saúde a que têm acesso*"[50].

No âmbito dos programas informáticos[51] e das bases de dados em ambiente hospitalar, cumpre referir que a disparidade e diversidade é bastante significativa, tendo em conta que muitas delas não são controladas pela instituição de saúde em si mesma, como por exemplo o S Clínico Hospitalar[52] da competência dos Serviços Partilhados do Ministério da Saúde, E.P.E., enquanto que outros têm gestão interna, como por exemplo um programa relativo ao transporte de doentes não urgentes ou mesmo gestão por parte de um subcontratante que controle um programa de exames de TAC[53].

[50] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;

[51] A este propósito EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE - *Handbook on European data protection law* – Luxemburgo, Publications office of the European union, 2018 "*A informação de saúde móvel é considerada como um campo emergente e em rápido crescimento, que tem o potencial de transformar a prestação de cuidados de saúde e melhorar a sua eficiência e qualidade*."

[52] http://spms.min-saude.pt/product/sclinicohospitalar "*O SClínico Hospitalar é um sistema de informação evolutivo, desenvolvido pela SPMS, que nasce da vasta experiência com duas anteriores aplicações usadas por milhares de médicos, enfermeiros e outros técnicos de saúde: o SAM (Sistema de Apoio ao Médico) e o SAPE (Sistema de Apoio à Prática de Enfermagem). Tem crescido para ser uma aplicação única, comum a todos os prestadores de cuidados de saúde e centrada no doente*."

[53] TAC - Tomografia axial computorizada

Para além das questões supra identificadas, os programas e aplicações informáticos que procedem ao tratamento de dados pessoais dos utentes têm ligação entre si, procedendo muitas vezes à transferência de dados para outros programas e outros locais de armazenamento, ou mesmo procedendo ao envio de dados de utentes do responsável pelo tratamento para outro responsável pelo tratamento[54].

A este propósito da transformação digital das entidades do Serviço Nacional de Saúde, destaco a pronúncia do Professor Henrique Martins, Presidente do Conselho de Administração dos Serviços Partilhados do Ministério da Saúde, E.P.E.[55], "*A transformação digital é hoje uma realidade na Sociedade em geral e nas Organizações em particular, com as tecnologias emergentes a potenciarem um conjunto de oportunidades de satisfação das necessidades das partes interessadas, de otimização dos recursos disponíveis e de otimização dos riscos relacionados. Neste contexto, a SPMS, EPE. tem vindo a acompanhar a inovação digital e a desenvolver um conjunto de iniciativas estratégias relacionadas com a melhoria da prestação dos serviços aos seus parceiros, a melhoria da eficiência organizacional e o lançamento de novos produtos e serviços digitais onde o fator inovação está fortemente presente. Conscientes de que este novo contexto digital acarreta um conjunto de novos cenários*

[54] Um exemplo de uma transferência de dados de um responsável de tratamento Hospital E.P.E. "A" para outro responsável pelo tratamento, também ele Hospital E.P.E. "B", é a necessidade de determinado utente estar internado num serviço do responsável pelo tratamento "A" e ser transferido para a realização de determinado exame ou intervenção clínica nas instalações do responsável pelo tratamento "B" e por conta deste, devendo para o correto desenrolar da intervenção e para a correta administração de cuidados de saúde, ser acompanhado de toda a informação clínica relevante, no âmbito daquela relação de prestação de cuidados de saúde.

[55] In http://spms.min-saude.pt/a-spms/ "*A SPMS – Serviços Partilhados do Ministério da Saúde, EPE tem a natureza de pessoa coletiva de direito público de natureza empresarial, dotada de personalidade jurídica, autonomia administrativa e financeira e de património próprio, nos termos do regime jurídico do setor empresarial do Estado, aprovado pelo Decreto-Lei n.º 133/2013, de 03 de outubro, estando sujeita à tutela dos membros do Governo responsáveis pelas áreas das finanças e da saúde. Foi criada em 2010, pelo Decreto-Lei n.º 19/2010, de 22 de março, alterado pelo Decreto-Lei n.º 108/2011, de 17 de novembro, pelo Decreto-Lei 209/2015, de 25 de setembro, e pelo Decreto-Lei 32/2016, de 28 de junho e pelo Decreto-Lei n.º 69/2017, de 16 de junho, tendo como missão a prestação de serviços partilhados – nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação – às entidades com atividade específica na área da saúde, de forma a "centralizar, otimizar e racionalizar" a aquisição de bens e serviços no Serviço Nacional de Saúde."*

de risco com impactos cada vez mais relevantes na operacionalidade das Organizações, a SPMS, EPE., em alinhamento com o previsto na Estratégia Nacional para o Ecossistema da Informação de Saúde 2020 (ENESIS2020), tem vindo a colocar os temas da Segurança de Informação, Cibersegurança e Privacidade dos dados no topo das suas preocupações, tendo lançado em 2016 o "Programa de Melhoria do Risco e Segurança da Informação", com o objetivo de promover a coordenação e partilha de boas práticas relacionadas com os sistemas de informação do Ministério da Saúde. Em 2017, as competências da SPMS, EPE no contexto da cibersegurança foram reforçadas com o Despacho nº1348/2017, em Diário da República nº28/2017, Série II de 2017-02-08, o qual identifica um conjunto de novas competências na coordenação, monitorização da implementação e operacionalização das boas práticas de melhoria contínua da resposta a ciber-riscos no setor da saúde."

Apesar do fenómeno da transformação digital e da preocupação com as matérias de cibersegurança estar bem patente, tanto nas instituições E.P.E. integrantes do SNS, como nos Serviços Partilhados do Ministério da Saúde, entidades que têm liderado esta matéria ao nível da área da saúde, a proteção de dados ao nível informático é apenas uma ponta do iceberg, no que diz respeito às matérias relativas à proteção de dados pessoais e da privacidade.

Pese embora toda a transformação digital existente nestas entidades tuteladas pelo ministério da saúde, não é menos verdade que uma quantidade considerável de informação relativa aos utentes, nomeadamente informação que contém dados relativos à saúde dos utentes, é tratada nas entidades pertencentes ao SNS através de procedimentos manuais, com recurso ao papel ou a meios básicos de informática.

Para além do supra exposto, também o fator humano inerente à prestação de cuidados de saúde e à consequente consulta de dados para a prestação de cuidados de saúde, que podem ir desde o momento de recolha de dados para a marcação de uma consulta de especialidade, passando pela realização de consulta e registo de dados e realização de exames, até à realização de um determinado procedimento cirúrgico durante o qual são recolhidos dados do utente sujeito à intervenção, sendo registados no processo clínico do utente, requer que os dados de saúde tenham uma proteção especial. Também nesse sentido indicam as disposições do manual sobre

proteção de dados da Agência Europeia para os Direitos Fundamentais, "*Os dados relativos à saúde estão sujeitos a um regime de processamento de dados mais restrito que os dados não sensíveis*"[56].

Como vimos, o tratamento de dados pessoais relativos à saúde de uma pessoa está intimamente ligado com a prestação de cuidados de saúde ministrados pelas entidades pertencentes ao SNS, sendo uma condição impossível de afastar e verdadeiramente acessória daquela prestação de cuidados.

Assim, e se bem que as preocupações em matéria de proteção de dados em Portugal, nomeadamente no setor da saúde, seriam à partida superiores às dos restantes setores, não menos verdade é que a publicação do Regulamento Geral de Proteção de Dados veio despertar na sociedade portuguesa em geral, e em particular nos profissionais ligados à área da saúde, uma consciência e um sentido crítico mais aguçados, o que leva a que muitas instituições tenham que efetuar alterações internas aos procedimentos instituídos, no sentido de mitigar riscos em matéria de violação de dados pessoais, que podem suscitar sanções previstas no regulamento ou mesmo eventuais ações de responsabilidade civil, com especial enfoque para estas últimas no âmbito do presente estudo, nunca devendo os responsáveis e os profissionais das entidades de saúde esquecer que a "*informação de saúde, incluindo os dados clínicos registados e outro exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa*"[57], assumindo aqui as instituições de saúde um papel de mero depositário dessa mesma informação clínica.

[56] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE - *Handbook on European data protection law* – Luxemburgo, Publications office of the European union, 2018;
[57] Artigo 3º da Lei n.º 12/2005, de 26 de janeiro

Capítulo II - O regime jurídico da proteção de dados pessoais

Neste capítulo abordarei o regime jurídico da proteção de dados pessoais no nosso país, no sentido de conseguirmos elencar um enquadramento geral acerca do que poderá estar em causa, em matéria de regulação de dados pessoais, em particular quando falamos de dados pessoais relativos à saúde, nomeadamente aqueles que são tratados e processados pelos hospitais e centros hospitalares portugueses.

1. Breves Considerações acerca da Lei n.º 67/98, de 26 de outubro

No presente momento, no nosso país, a Lei n.º 67/98, de 26 de outubro continua a ser a lei portuguesa em matéria de proteção de dados. Como já vimos, esta lei transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24/10/95, contendo em grande parte as disposições constantes no novo Regulamento Geral de Proteção de Dados, sem prejuízo das novas disposições e instrumentos deste diploma, que analisarei em seguida.

A este propósito, cumpre citar o comunicado da Autoridade de Controlo portuguesa em matéria de proteção de dados, a Comissão Nacional de Proteção de Dados[58], emitido no dia 25 de maio de 2018, que explicitou que enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98 de 26 de outubro, esta lei se mantém em vigor em tudo o que não contrarie o Regulamento.

Mais explicitou aquele comunicado[59], que no que diz respeito ao tratamento de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º

[58] Lei nº 43/2004 de 18 de Agosto - Lei de funcionamento da CNPD

[59] Comunicado da CNPD - Aplicação do novo quadro legal de proteção de dados, de 25 de maio de 2018 "…A partir de hoje, 25 de maio de 2018, o RGPD tem plena aplicação em toda a União Europeia e, por isso, também em Portugal. Enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98, de 26 de outubro, esta lei manter-se-á em vigor em tudo o que não contrarie aquele diploma europeu. No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680…"

67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680[60].

2. Conceito de dados pessoais à luz da Lei n.º 67/98

Chegados a esta fase, é importante percebermos à luz da Lei n.º 67/98 de 26 de Outubro, o que se entende por dados pessoais.

Assim, estipula a al. a) do artigo 3º da Lei n.º 67/98 de 26 de Outubro, que se entende por dados pessoais "*qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*".

[60] Diretiva (EU) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

Capítulo III - O Regulamento Geral de Proteção de Dados da UE

O Regulamento Geral de Proteção de Dados da União Europeia 2016/679[61], estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na União Europeia.

Este Regulamento, que entrou em vigor no dia 24 de maio de 2016 e que é de aplicação direta em todos os Estados Membros da União Europeia, desde o dia 25 de maio de 2018, não se aplica ao tratamento de dados pessoais de pessoas falecidas ou de pessoas coletivas.

O Regulamento não se aplica também ao tratamento de dados pessoais por motivos exclusivamente pessoais ou no exercício de atividades domésticas, desde que não haja qualquer ligação com uma atividade profissional ou comercial.

O novo Regulamento Geral de Proteção de Dados trouxe uma autêntica mudança de paradigma, no que diz respeito ao tratamento de dados pessoais de cidadãos da União Europeia, apesar de não ser correto afirmar que o Regulamento traga só por si novos direitos e novos deveres, no que diz respeito ao tratamento de dados pessoais, tendo em conta que grande parte das suas exigências se encontravam já plasmadas na Diretiva 95/46/CE[62].

Como vimos anteriormente, a Diretiva 95/46/CE foi transposta para o ordenamento jurídico português pela Lei n.º 67/98, de 26 de outubro, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, sendo que já neste diploma eram estipuladas algumas regras de grande semelhança, ao que se encontra previsto no Regulamento Geral de Proteção de Dados.

---

[61] 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

[62] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24.10.1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Consultar em *http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:01995L0046-20031120&from=EN*

O RGPD acarreta sim uma panóplia de novidades em matéria de proteção de dados pessoais, que se traduzem em alguns novos princípios e conceitos, alguns novos direitos para os titulares de dados pessoais e novos deveres para as entidades que tratam esses dados, razão pela qual as entidades que procedem ao tratamento de dados de categorias especiais, particularmente protegidos em sede de Regulamento Geral de Proteção de Dados, devem acautelar as necessárias adaptações no âmbito do tratamento de dados pessoais.

1. Conceitos do Regulamento Geral de Proteção de Dados

Para entendermos as disposições relativas à proteção de dados pessoais, de acordo com o que se encontra disposto no Regulamento Geral de Proteção de Dados, importa aferir aqueles que são os conceitos mais relevantes, plasmados no artigo 4º do regulamento. Assim, destacamos os seguintes, com especial relevância para o nosso estudo:

- Dados Pessoais, é toda a "*informação relativa a uma pessoa singular identificada ou identificável, sendo que para o efeito se considera identificável 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*". No caso específico da saúde, deveremos ter especial atenção à definição de dados pessoais relativos à saúde[63];
- Tratamento define-se como "*uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de 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*

[63] A este propósito, ver a interpretação do Grupo de Trabalho do Artigo 29º, contida no "*Parecer 4/2007 sobre o conceito de dados pessoais*".

qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". Um exemplo de tratamento ao nível dos Hospitais e Centros Hospitalares é o registo de informação clínica relativa ao utente, no sistema informático S Clínico;

- Limitação do tratamento consiste na " *inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro*";
- Definição de Perfis, consiste em "*qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações*";
- Pseudonomização consiste no "*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*". Esta técnica poderá ser muito útil na realidade dos Hospitais e Centros Hospitalares, como veremos no capítulo referente à implementação de um sistema de gestão de dados pessoais, como proposta de solução ao problema identificado. A título de exemplo, aos processos clínicos que circulam internamente na instituição para efeitos de realização de auditorias, pode ser aplicada a técnica da pseudonomização, na medida em que o profissional que irá realizar o estudo, não necessita saber o nome do utente a que corresponde o processo clínico;
- Ficheiro é "*qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico*". Podemos estar a falar de uma tabela em Excel, contendo dados relativos a utentes, guardada no computador de secretária de um funcionário, ou mesmo guardados no correio eletrónico profissional;

- Responsável pelo Tratamento define-se como "*a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro*". Para o efeito, responsável pelo tratamento é, por exemplo, o hospital ou centro hospitalar E.P.E.;
- Subcontratante é "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*". Os Hospitais recorrem diversas vezes a entidades subcontratantes para a prestação adequada de cuidados de saúde. Um exemplo de uma entidade subcontratante é por exemplo uma empresa que preste serviços de realização de exames de TAC ou de Ressonância Magnética por conta do Hospital, tratando dados dos utentes do Hospital por conta deste, com a finalidade última de prestar os adequados cuidados de saúde;
- Destinatário é "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento*". No âmbito das prestações de cuidados de saúde, existem destinatários que recebem dados enviados pelo responsável pelo tratamento. Um exemplo de destinatário será uma outra entidade do Serviço Nacional de Saúde que receba os dados do utente, que venha a ser sujeito a uma intervenção nessa mesma entidade destinatária;
- Terceiro é "*a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o*

subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais";

- Consentimento do titular dos dados consiste numa "*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*". O consentimento é um dos requisitos de licitude para o tratamento dos dados pessoais, porém, não deverá ser aquele em que assenta o tratamento de dados relativos à saúde, no âmbito da prestação de cuidados de saúde no SNS[64];
- Violação de Dados Pessoais é "*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*". Uma violação de dados pessoais pode ser um ataque informático, uma fotografia publicada numa rede social contendo informação relativa a um titular dos dados sem autorização, ou mesmo um furto de um equipamento que contenha informação relativa a titular de dados, como um telemóvel, um computador ou um dispositivo de armazenamento portátil;
- Dados Relativos à saúde são "*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*". Veremos em detalhe esta questão no ponto seguinte, relativo aos dados pessoais em saúde à luz do RGPD;
- Autoridade de Controlo é "*uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51º*" do Regulamento. No caso de Portugal, a autoridade de controlo nacional é a Comissão Nacional de Proteção de Dados[65].

[64] A este propósito, consultar as exceções de tratamento de dados de categoria especial, nos termos do n.º2 do artigo 9º do RGPD.
[65] A este propósito, consultar o artigo 3º da proposta de Lei n.º 120/XIII

2. Princípios do artigo 5º do RGPD

O artigo 5º do RGPD estabelece aqueles que devem ser os princípios relativos ao tratamento de dados pessoais, nomeadamente o princípio da licitude, lealdade e transparência, o princípio da limitação das finalidades, o princípio da minimização dos dados, o princípio da exatidão, o princípio da limitação da conservação, o princípio da integridade e confidencialidade e o princípio da responsabilidade. Nesta medida, cada princípio estabelece o seguinte:

- Princípio da licitude, lealdade e transparência, serve para garantir que os dados pessoais serão sempre objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados pessoais;
- Princípio da limitação das finalidades é o princípio que garante que os dados pessoais são sempre recolhidos para determinada finalidade, finalidade essa que deve ser explícita e legítima. Este princípio estabelece que os dados pessoais recolhidos não podem posteriormente e de uma forma incompatível com essas finalidades, ser de novo tratados. Mais, estabelece este princípio, que no caso de o tratamento posterior à finalidade inicial ser necessário para fins de arquivo de interesse público, ou para fins de investigação científica ou histórico ou para fins estatísticos, este tratamento não será considerado incompatível, desde que cumprido o disposto no artigo 89º, n.1;
- Princípio da minimização dos dados, garante que os dados recolhidos são os adequados, pertinentes e limitados ao que é necessário, relativamente às finalidades para as quais são tratados;
- Princípio da exatidão, estabelece que os dados tratados são exatos e que são alvo de atualização sempre que necessário, devendo ao mesmo tempo ser adotadas todas as medidas adequadas para que os dados considerado inexatos, sejam apagados ou retificados;
- Princípio da limitação da conservação, garante que os dados que se encontram a tratamento pelo responsável pelo tratamento, apenas permite a identificação dos titulares desses mesmos dados, estritamente pelo período que seja necessário para as finalidades para as quais os mesmos são tratados. No caso de os dados serem necessários para fins de arquivo, nos termos do

artigo 89º, n.º1, devem os mesmos serem sujeitos à aplicação de medidas técnicas e organizativas adequadas nos termos do RGPD, de forma a salvaguardar os direitos e liberdades do titular dos dados;

- Princípio da integridade e confidencialidade, estabelece que os dados pessoais devem ser tratados de uma forma que garanta a segurança dos dados, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a perda desses dados, contra a destruição ou danificação acidental, devendo o responsável pelo tratamento adotar as medidas técnicas ou organizativas adequadas para proteger esses dados;
- Princípio da responsabilidade, estabelece que o responsável pelo tratamento é responsável pelo cumprimento dos princípios supra referidos, tendo a obrigação de comprovar o cumprimento, demonstrando perante o titular, a autoridade de controlo ou outro organismo o cumprimento dos princípios.

O princípio da responsabilidade ou princípio da responsabilidade demonstrável é um dos princípios fundamentais de sustentação do RGPD e um dos princípios basilares para o tratamento de dados pessoais, por parte dos responsáveis pelo tratamento.

Como veremos em seguida, o RGPD oferece às instituições um conjunto de ferramentas, algumas delas de implementação ou designação obrigatória, que permitem precisamente aos responsáveis pelo tratamento demonstrar a conformidade com o RGPD, nomeadamente a figura do Encarregado de Proteção de Dados, a obrigação de registo das operações de tratamento, as Avaliações de Impacto sobre a proteção de dados, o estabelecimento e divulgação de políticas de privacidade ou a implementação de códigos de conduta internos. Não obstante, veremos em maior detalhe como estes instrumentos podem ser utilizados pelo responsável pelo tratamento para cumprir com o princípio da responsabilidade demonstrável, fator de maior relevância no âmbito do nosso estudo, dada a problemática da responsabilidade civil do responsável pelo tratamento.

3. Conceito de dados pessoais em saúde à luz do RGPD

De acordo com o estipulado no Regulamento Geral de Proteção de Dados, nomeadamente no artigo 9º com a epígrafe "*Tratamento de categoriais especiais de dados pessoais*", os dados pessoais relativos à saúde de uma pessoa são considerados dados de categoria especial[66], podendo ser definidos como dados especiais.

Neste âmbito, será pertinente atender aos considerandos *51 a 54* do Regulamento Geral de Proteção de Dados, onde se encontra plasmado que "*Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais",* sendo que com já vimos, os dados pessoais relativos à saúde, merecem uma especial proteção dada a sensibilidade dos mesmos. Devem ainda ser previstas " *de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso".*

É ainda que estabelecido que para as categorias especiais de dados pessoais *"que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público…"*[67]*.*

[66] A este propósito, ver a Lei n.º 12/2005, de 26 de Janeiro, sobre a Informação Genética Pessoal e Informação de Saúde, que define o conceito de informação de saúde e de informação genética, a circulação de informação e a intervenção sobre o genoma humano no sistema de saúde, bem como as regras para a colheita e conservação de produtos biológicos para efeitos de testes genéticos ou de investigação.
[67] Sublinhado nosso.

Encontra-se ainda previsto que o RGPD estabeleça *"condições harmonizadas para o tratamento de categorias especiais de dados pessoais relativos à saúde, tendo em conta necessidades específicas, designadamente quando o tratamento desses dados for efetuado para determinadas finalidades ligadas à saúde por pessoas sujeitas a uma obrigação legal de sigilo profissional."*

Ainda de acordo com o artigo 7º, n.º1 da Lei n.º 67/98, de 26 de outubro, os dados relativos à saúde de uma pessoa são considerados dados sensíveis, sendo à partida o seu tratamento proibido por defeito, apesar de existirem algumas condições de licitude para o seu tratamento, com que nos conduz no mesmo sentido que o RGPD.

No entendimento de Sérgio Deodato dados pessoais em saúde são "*dados pessoais relativos à saúde de uma pessoa e que normalmente são recolhidos, registados e usados pelos profissionais de saúde*"[68].

4. Tratamento de dados pessoais em saúde

Uma das questões mais pertinentes no âmbito das atividades desenvolvidas por uma instituição de saúde é precisamente o tratamento de dados pessoais relativos à saúde de uma pessoa.

Com efeito, apesar da atividade principal de um Hospital ser a prestação de cuidados de saúde, é praticamente impossível de afastar que a prestação de cuidados de saúde tem que invariavelmente estar acompanhada pelo tratamento de dados pessoais dos utentes, para uma adequada prestação de cuidados, atendendo naturalmente ao historial clínico dos doentes, por forma à tomada de decisões com uma maior segurança clínica.

As instituições de saúde são aquelas que mais se devem preocupar com o adequado e correto tratamento de dados, tendo em conta que, como já vimos, os dados pessoais em saúde são dados considerados como pertencentes a categorias

[68] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;

especiais, devendo as instituições de saúde acautelar a sua devida proteção e não divulgação, na medida em que, como defende o autor Sérgio Deodato os dados de saúde "*quando são partilhados – revelados ou expostos – para fora da fronteira individual, passam a ser conhecidos pelos profissionais de saúde, o que não significa que passem para o espectro público*"[69].

Nos termos do artigo 9º, onde o tratamento de dados pessoais relativos à saúde de uma pessoa é considerado, por defeito, proibido, são consagradas algumas exceções que afastam essa proibição de tratamento.

Nestes termos, o tratamento de dados pessoais relativos à saúde de uma pessoa não é proibido nos seguintes casos, entre outros devidamente identificados no n.º 2 do artigo 9º:

- *Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados;*
- *Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;*
- *Se 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;*
- *Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;*
- *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser*

[69] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;

proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

- *Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;*
- *Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;*
- *Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.*

Ora, para a prestação de cuidados de saúde é importante destacar as disposições constantes nas alíneas c), nomeadamente no caso do tratamento de dados relativos à saúde de uma pessoa ser necessário para a proteção dos interesses vitais do titular dos dados (neste caso o utente) ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento e particularmente a alínea h), quando o tratamento de dados relativos à saúde do

utente seja necessário para a prestação de cuidados ou tratamentos de saúde ou de ação social, ou para a gestão de sistemas e serviços e saúde ou de ação social.

Neste âmbito não poderá nunca ser afastada a disposição do n.º3 do artigo 9º[70], que estabelece que "*os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes*.", o que nos leva a concluir que os dados pessoais de saúde, para o efeito da prestação de cuidados de saúde, têm obrigatoriamente que ser tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional[71].

Para além da disposição constante no Regulamento Geral de Proteção de Dados relativa ao tratamento de dados pessoais de categorias especiais, cumpre ainda atender à estipulação do n.º5 do artigo 11 da Lei n.º 67/98 de 26 de outubro, que estipula que "*o tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27.º, e sejam garantidas medidas adequadas de segurança da informação*", o que nos conduz no mesmo sentido do disposto do RGPD.

[70] Disposição do n.º3 do artigo 9º do RGPD, sobre a obrigatoriedade dos dados relativos à saúde serem tratados por profissional sujeito a obrigação de sigilo profissional.
[71] A este propósito DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017 "*Ao tomarem contacto com esta informação, os profissionais de saúde ficam imediatamente obrigados ao dever de guardar segredo, através do dever deontológico de sigilo* profissional… Atualmente, todas as profissões reguladas da saúde têm inscrito nas suas deontologias profissionais, o dever de sigilo".

5. Encarregado de Proteção de Dados

O Regulamento Geral de Proteção de Dados trouxe algumas novidades no que diz respeito às funções profissionais, prevendo uma nova figura relativa ao tratamento e à proteção de dados pessoais, nomeadamente o Encarregado de Proteção de Dados.

O Encarregado de Proteção de Dados é uma figura que não se encontrava prevista na antiga Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, 24/10/95, nem tão pouco na Lei n.º 67/98 de 26 de outubro, pese embora seja obrigatória para determinado tipo de empresas e entidades, como veremos em seguida.

A figura do Encarregado de Proteção de Dados encontra-se prevista nos artigos 37º, 38º e 39º do Regulamento Geral de Proteção de Dados, prevendo estes artigos, respetivamente, a forma de designação do Encarregado de Proteção de Dados, a posição do Encarregado de Proteção de Dados dentro da instituição e as funções do Encarregado de Proteção de Dados.

Neste âmbito, importa aferir que tipo de entidades estão obrigadas, à luz do Regulamento Geral de Proteção de Dados, a designar esta figura, conseguindo perceber que, por diversas razões, as instituições de saúde e em particular os Hospitais E.P.E. são obrigados a designar um Encarregado de Proteção de Dados.

Com efeito, o Regulamento Geral de Proteção de Dados, no n.º1 do artigo 37º prevê que o responsável pelo tratamento e o subcontratante designem um Encarregado de Proteção de Dados, sempre que:

a) *O tratamento for efetuado por uma autoridade ou um organismo público*[72], *excetuando os tribunais no exercício da sua função jurisdicional;*

[72] Grupo de Trabalho do Artigo 29 – Orientações sobre o Encarregado de Proteção de Dados - "*O RGPD não define o que constitui «uma autoridade ou um organismo público». O GT 29 considera que este conceito deve ser definido ao abrigo da legislação nacional. Por conseguinte, as autoridades e organismos públicos incluem as autoridades nacionais, regionais e locais, mas o seu conceito, nos termos das legislações nacionais aplicáveis, também engloba, por norma, um conjunto de outros organismos de direito público. Nestes casos, a designação de um EPD é obrigatória*."

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

c) *As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º.*

Neste âmbito, se é líquido que um Hospital com a natureza de Entidade Pública Empresarial tem que designar um Encarregado de Proteção de Dados por assumir a forma de organismo público, não será de afastar a aferição da necessidade de designação desta figura, recorrendo às alíneas b) e c), pelas razões que passo a enunciar.

As entidades estão obrigadas a designar um Encarregado de Proteção de Dados sempre que as atividades do responsável pelo tratamento consistirem em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala. Ora, se bem que a atividade principal dos Hospitais E.P.E. e dos restantes Hospitais é a prestação de cuidados de saúde, como já vimos, a prossecução desta atividade não é possível sem que exista um tratamento de dados dos titulares dos dados em grande escala[73], razão pela qual também estão os Hospitais E.P.E. obrigados a designar um Encarregado de Proteção de Dados.

[73] Grupo de Trabalho do Artigo 29 – Orientações sobre o Encarregado de Proteção de Dados – "*O artigo 37.º, n.º 1, alíneas b) e c), do RGPD faz referência às «atividades principais do responsável pelo tratamento ou do subcontratante». O considerando 97 especifica que as atividades principais do responsável pelo tratamento dizem respeito às suas «atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar». As «atividades principais» podem entender-se como as operações essenciais necessárias para alcançar os objetivos do responsável pelo tratamento ou do subcontratante. No entanto, a interpretação das «atividades principais» não deve excluir as atividades em que o tratamento de dados constitui uma parte indissociável das atividades do responsável pelo tratamento ou do subcontratante. Por exemplo, a atividade principal de um hospital é a prestação de cuidados de saúde. Contudo, um hospital não poderia prestar cuidados de saúde de forma segura e eficaz sem proceder ao tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes. Assim, o tratamento destes dados deve ser*

Por fim, atendendo à al. c) do n.º1 do artigo 37º, também aquelas entidades cujas atividades principais do responsável pelo tratamento consistam em operações de tratamento em grande escala[74] de categorias especiais de dados nos termos do artigo 9º do regulamento, estão obrigados a designar um Encarregado de Proteção de Dados, o que manifestamente também é o caso dos Hospitais E.P.E., tendo em conta que na prossecução da sua atividade principal, a prestação de cuidados de saúde, procedem ao tratamento em grande escala de categorias especiais de dados de categorias especiais, como é o caso dos dados pessoais relativos à saúde de uma pessoa.

Relativamente à modalidade de designação, o Regulamento Geral de Proteção de Dados prevê que o Encarregado de Proteção de Dados possa ser designado por grupo empresarial desde que haja um encarregado de proteção de dados acessível a partir de cada estabelecimento, ou no caso do responsável pelo tratamento ser um organismo público, poderá também ser designado um único encarregado de proteção de dados para vários desses organismos públicos, atendendo à estrutura organizacional e dimensão.

Apesar de o RGPD não prever nenhuma característica especial para o desempenho da função de Encarregado de Proteção de Dados, prevê o n.º 5 do artigo 37º que o encarregado da proteção de dados é 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, bem como na sua capacidade para desempenhar as funções referidas no artigo 39º. Esta disposição é vaga e abstrata, tendo em conta que o Regulamento não densifica o que para o efeito devem ser considerados conhecimento especializados no domínio do direito, nem tão pouco o

considerado uma das atividades principais de qualquer hospital, cabendo, portanto, aos hospitais nomear encarregados da proteção de dados."

[74] Grupo de Trabalho do Artigo 29 – Orientações sobre o Encarregado de Proteção de Dados – "*O GT 29 recomenda que, em especial, os seguintes fatores sejam tomados em consideração para determinar se o tratamento é efetuado em grande escala: O número de titulares de dados afetados – como número concreto ou em percentagem da população em causa; O volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento; A duração, ou permanência, da atividade de tratamento de dados; O âmbito geográfico da atividade de tratamento... Contam-se como exemplos de tratamento de grande escala: o tratamento de dados de doentes no exercício normal das atividades de um hospital*"

que se devem considerar domínio de práticas de proteção de dados. Outro conceito vago e indeterminado que o Regulamento Geral de Proteção de Dados nos oferece, tem que ver com a previsão da capacidade para desempenhar as funções do encarregado, previstas no artigo 39º do RGPD, o que poderá dificultar a escolha da pessoa que irá desempenhar a função.

Para além de tudo o já referido, o encarregado de proteção de dados pode ser designado internamente na instituição, com a designação de um trabalhador dos quadros internos da empresa, ou pode ser contratado através de um contrato de prestação de serviços, desempenhando as funções externamente.

A função do Encarregado de Proteção de Dados pressupõe uma especial posição dentro da organização, nomeadamente tendo em conta a necessidade de envolver esta figura em todas as questões relacionadas com a proteção de dados pessoais.

No desempenho da sua função, o Encarregado de Proteção de Dados tem que ter acesso aos recursos necessários para o desempenho da sua função, tendo que lhe ser dadas condições para manter os seus conhecimentos, bem como tem que ter acesso aos dados pessoais e às operações de tratamento das instituições.

Neste âmbito, importa referir a necessidade de garantir a independência e imparcialidade do Encarregado de Proteção de Dados no desempenho das suas funções, prevendo o n.º3 do artigo 38º que o responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções, não podendo ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções, exercendo aqui o Regulamento Geral de Proteção de Dados uma função de salvaguarda do profissional que venha a desempenhar a função, por não ser penalizado por exercer as funções que lhe estão previstas.

Mais, prevê o regulamento que o encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante, tendo em conta que no desempenho das suas funções o encarregado poderá ter que realizar auditorias às operações de tratamento levadas a cabo por determinados serviços, tendo inclusivamente que emitir pareceres sobre

determinadas operações de tratamento, não fazendo sentido de que no desempenho dessa função, esteja subordinado a um superior hierárquico que, no limite, tenha que vir a ser fiscalizado por si, o que colocaria o encarregado de proteção de dados numa posição de pouca autonomia e com limitação no desempenho das suas funções.

O RGPD prevê ainda que a função de Encarregado de proteção de dados possa ser exercida através da acumulação de funções, nomeadamente com funções que não sejam incompatíveis. A este propósito, o Grupo de Trabalho do artigo 29º considera como funções incompatíveis, nomeadamente as seguintes[75]: diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático.

Relativamente às funções do Encarregado de Proteção de Dados, estipula o artigo 39º que esta figura tem, nomeadamente, as seguintes funções:

- *Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;*
- *Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;*

[75] Grupo de Trabalho do Artigo 29 – Orientações sobre o Encarregado de Proteção de Dados – "*Regra geral, os cargos suscetíveis de gerar conflitos no seio da organização podem incluir não só os cargos de gestão superiores (por exemplo, diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático), mas também outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento. Além disso, pode igualmente surgir um conflito de interesses se, por exemplo, um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados*."

- *Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º;*
- *Coopera com a autoridade de controlo;*
- *Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.*

Assim, o Encarregado de Proteção de Dados funciona como um pilar de responsabilidade dentro da instituição, sendo um excelente incentivo no caminho para a conformidade com o Regulamento Geral de Proteção de Dados, na medida em que garante que as instituições, nomeadamente os Hospitais E.P.E., tenham nos seus quadros algum funcionário permanentemente preocupado com as questões relativas à privacidade e à proteção de dados pessoais.

Entre as funções de maior importância, estão naturalmente aquelas que se prendem com o acompanhamento e aconselhamento permanente do responsável pelo tratamento e dos titulares dos dados, bem como o facto de ter que ser um ponto de contacto permanente com a Comissão Nacional de Proteção de Dados para as questões de privacidade da instituição em que está inserido. Outra função de extrema relevância, tem que ver com a realização de auditorias relativas à proteção de dados pessoais, o que garante um acompanhamento constante e uma verdadeira integração dos diversos serviços das instituições nestas matérias da proteção de dados.

Deste modo, a figura do Encarregado de Proteção de Dados poderá ser visto como um garante de conformidade e como parte de uma solução que venha a mitigar os riscos em matéria de violação de dados pessoais, como veremos em seguida.

Ainda assim, é importante que se tenha sempre presente que o Encarregado de Proteção de Dados não é pessoalmente responsável em caso de incumprimento ou de violação de dados que eventualmente ocorra, caindo essa responsabilidade sempre na esfera do Responsável pelo Tratamento, nos termos do n.º2 do artigo 82º

do regulamento, onde se encontra plasmado que "*Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento*".

6. Registo das Atividades de Tratamento de Dados

Uma das obrigações com maior relevância, no âmbito da aplicação do RGPD, tem precisamente que ver com a obrigação de registo das operações de tratamento de dados, obrigação essa que recai sobre o Responsável pelo Tratamento, nomeadamente no caso de se tratar de um Hospital ou Centro Hospitalar E.P.E., pelas razões que veremos em seguida.

Com efeito, estabelece o n.º5 do artigo 30º do RGPD que as empresas ou entidades que tenham no seu quadro de pessoal mais de 250 trabalhadores, ou aquelas empresas ou entidades que procedam ao tratamento de dados que seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, ou nomeadamente com particular interesse para o nosso estudo, que o tratamento efetuado abranja dados de categoriais especiais, como é o caso dos dados relativos à saúde de uma pessoa, são obrigadas a proceder ao registo das atividades de tratamento de dados.

Nos termos do n.º1 do artigo 30º do RGPD, o registo conservado pelo responsável do tratamento deve conter as seguintes informações:

- *O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;*
- *As finalidades do tratamento dos dados;*
- *A descrição das categorias de titulares de dados e das categorias de dados pessoais;*
- *As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;*

- *Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;*
- *Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;*
- *Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1.*

Esta obrigação de registo das atividades de tratamento recai igualmente sobre o subcontratante, nomeadamente no caso de subcontratantes que para um Hospital ou Centro Hospitalar tratem dados de utentes, por conta daqueles responsáveis pelo tratamento, devendo esses subcontratantes conservar um registo de todas as categorias de atividades de tratamento realizadas em nome do responsável pelo tratamento, do qual constará:

- *O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;*
- *As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento;*
- *Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;*
- *Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1.*

Importa ressalvar que o registo das operações de tratamento terá obrigatoriamente que ser efetuado por escrito, podendo naturalmente o registo ser feito por escrito, em formato eletrónico.

No âmbito do registo das operações de tratamento de dados, importa efetuar uma remissão para o n.º1 do artigo 24º, relativo à responsabilidade do responsável pelo tratamento, nomeadamente o facto de este ter que aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD, sendo que na minha opinião, o registo sobre as operações de tratamento de dados, uma ferramenta bastante útil no sentido de demonstrar perante a autoridade de controlo e perante o próprio titular dos dados o cumprimento com o disposto no RGPD.

7. Autoridade de Controlo Nacional

No âmbito do nosso estudo considero absolutamente fundamental efetuar um breve enquadramento acerca da autoridade de controlo do nosso país, nomeadamente aquela que terá a atribuição de exercer os poderes de fiscalização em matéria de proteção de dados pessoais, sendo o garante da aplicação do RGPD e das políticas de proteção de dados pessoais em Portugal.

Com efeito, a autoridade de controlo nacional em matéria de proteção de dados tem sido, até ao momento, a Comissão Nacional de Proteção de Dados[76].

Nos termos da Lei n.º 43/2004 de 18 de Agosto "*A CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República, com as atribuições e competências definidas na lei*."

Na Lei n.º 67/98 de 26 de outubro, a lei de proteção de dados pessoais ainda em vigor, a CNPD encontra-se prevista no Capítulo IV, estabelecendo o artigo 22º daquele diploma legal, aquelas que são das suas atribuições, nomeadamente "*controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei*."

De acordo com o disposto nas alíneas do n.º3 do artigo 22º, a CNPD dispõe de:

[76] Lei n.º 43/2004 de 18 de Agosto - Regula a organização e o funcionamento da Comissão Nacional de Proteção de Dados (CNPD), bem como o estatuto pessoal dos seus membros.

"a) *De poderes de investigação e de inquérito, podendo aceder aos dados objeto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo*

b) De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português

c) Do poder de emitir pareceres prévios ao tratamento de dados pessoais, assegurando a sua publicitação."

Neste seguimento, atendemos ao disposto no artigo 23º da Lei 67/98, nomeadamente aquelas que são as competências da CNPD:

a) *"Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais;*
b) *Autorizar ou registar, consoante os casos, os tratamentos de dados pessoais;*
c) *Autorizar excecionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5.º;*
d) *Autorizar, nos casos previstos no artigo 9.º, a interconexão de tratamentos automatizados de dados pessoais;*
e) *Autorizar a transferência de dados pessoais nos casos previstos no artigo 20.º;*
f) *Fixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir diretivas para determinados sectores de atividade;*
g) *Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de retificação e atualização;*
h) *Autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, bem como fixar os prazos máximos de cumprimento, em cada sector de atividade, das obrigações que, por força dos artigos 11.º a 13.º, incumbem aos responsáveis pelo tratamento de dados pessoais;*

i) Dar seguimento ao pedido efetuado por qualquer pessoa, ou por associação que a represente, para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais e informá-la do resultado;

j) Efetuar, a pedido de qualquer pessoa, a verificação de licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;

k) Apreciar as reclamações, queixas ou petições dos particulares;

l) Dispensar a execução de medidas de segurança, nos termos previstos no n.º 2 do artigo 15.º, podendo emitir diretivas para determinados sectores de atividade;

m) Assegurar a representação junto de instâncias comuns de controlo e em reuniões comunitárias e internacionais de entidades independentes de controlo da proteção de dados pessoais, bem como participar em reuniões internacionais no âmbito das suas competências, designadamente exercer funções de representação e fiscalização no âmbito dos sistemas Schengen e Europol, nos termos das disposições aplicáveis;

n) Deliberar sobre a aplicação de coimas;

o) Promover e apreciar códigos de conduta;

p) Promover a divulgação e esclarecimento dos direitos relativos à proteção de dados e dar publicidade periódica à sua atividade, nomeadamente através da publicação de um relatório anual;

q) Exercer outras competências legalmente previstas."

Não obstante as competências supra referidas nesta lei de 1998, considero pertinente auscultar as disposições constantes na proposta de lei do governo n.º 120/XIII[77]. Assim, o artigo 3º[78] vem prever que a CNPD será a Autoridade de

[77] Proposta de Lei n.º 120/XIII - http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true

[78] Pese embora não seja oficial, de acordo com o disposto na proposta de lei n.º 120/XIII, a Comissão Nacional de Proteção de Dados será a autoridade nacional de controlo, no nosso país.

Controlo Nacional, nos termos do RGPD, bem como nos termos da futura lei. Mais, cumpre aferir aquelas que serão as novas atribuições da CNPD, constantes no n.º1 do artigo 6º, sendo que competirá à CNPD:

"a) Pronunciar-se, a título não vinculativo, sobre as medidas legislativas e regulamentares relativas à proteção de dados pessoais, bem como sobre instrumentos jurídicos em preparação, em instituições europeias ou internacionais, relativos à mesma matéria;

b) Fiscalizar o cumprimento das disposições do RGPD e das demais disposições legais e regulamentares relativas à proteção de dados pessoais e dos direitos, liberdades e garantias dos titulares dos dados, e corrigir e sancionar o seu incumprimento;

c)Disponibilizar uma lista de tratamentos sujeitos à avaliação do impacto sobre a proteção de dados, nos termos do n.º 4 do artigo 35.º do RGPD, definindo igualmente critérios que permitam densificar a noção de elevado risco prevista nesse artigo;

d) Elaborar e apresentar ao Comité Europeu para a Proteção de Dados, previsto no RGPD, os projetos de critérios para a acreditação dos organismos de monitorização de códigos de conduta e dos organismos de certificação, nos termos dos artigos 41.º e 43.º do RGPD, e assegurar a posterior publicação dos critérios, caso sejam aprovados;

e)Acreditar organismos para monitorizar códigos de conduta, nos termos do RGPD, bem como revogar a acreditação sempre que os requisitos deixem de ser cumpridos ou as medidas adotadas violem as normas de proteção de dados;

f)Cooperar com o Instituto Português de Acreditação, I.P. (IPAC, I.P.), relativamente à aplicação do disposto no artigo 14.º da presente lei, bem como na definição de requisitos adicionais de acreditação, tendo em vista a salvaguarda da coerência de aplicação do RGPD;

g) Promover ações de formação adequadas e regulares destinadas aos encarregados de proteção de dados."

Para além das disposições atuais e futuras do direito interno, as disposições relativas à autoridade de controlo estão previstas nos artigos 55º e ss. do RGPD.

Conforme resulta da análise das competências, atribuições e poderes da autoridade de controlo e nomeadamente atendendo aquelas que eram as competências da CNPD antes da aplicação direta do RGPD na UE, é possível verificar que se deu uma inversão no paradigma que passou a ser autorregulatório, no sentido em que, a CNPD deixou de ter poderes de concessão de autorização prévia (ou de comunicação obrigatória de tratamento de dados), como por exemplo para a instalação de câmaras de videovigilância nas instalações de determinado responsável pelo tratamento, recaindo agora sobre o responsável pelo tratamento a obrigação de efetuar uma *Avaliação de Impacto sobre a Proteção de Dados*[79] a essa operação de tratamento de dados em concreto, analisando os eventuais riscos a que os titulares dos dados pessoais possam estar sujeitos e concluir se existe ou não risco para os titulares dos dados, e bem assim, adotar as medidas de mitigação que considere pertinentes para eliminar ou ultrapassar os riscos identificados[80].

Neste âmbito, as notificações à autoridade de controlo deixam de ser necessárias, sendo sim necessário que o responsável pelo tratamento adote medidas e procedimentos em conformidade com o RGPD e que nesse sentido, tenha capacidade de demonstrar perante os titulares dos dados, perante a CNPD e perante os tribunais, que cumpre as normas em matéria de proteção de dados pessoais.

[79] AIP - Avaliação de Impacto sobre a Proteção de Dados

[80] Neste caso em concreto, o responsável pelo tratamento tem a obrigação de consultar a autoridade de controlo antes de proceder ao tratamento dos dados pessoais, sempre que da AIP se concluir que o tratamento de dados resultaria num elevado risco na ausência de medidas de mitigação tomadas pelo responsável pelo tratamento para atenuar o risco dos titulares, nos termos do disposto no n.º1 do artigo 36º do RGPD.

PARTE III – VULNERABILIDADE E PROPOSTA DE SOLUÇÃO

Capítulo I - Responsabilidade Civil do Responsável pelo Tratamento por violação de Proteção de Dados Pessoais

Como foi possível aferir até esta fase do nosso estudo, o universo dos Hospitais e Centros Hospitalares portugueses que integram o Serviço Nacional de Saúde e aquelas que são as suas particularidades em matéria de utilização de dados pessoais para a prossecução daquelas que são as suas legítimas funções poderá acarretar diversos riscos para os titulares dos dados pessoais e em particular dos dados pessoais relativos à saúde, bem como para as instituições de saúde[81].

De entre os elevados riscos em matéria de proteção de dados pessoais, podemos catalogar determinadas ocorrências como violação de dados pessoais. Como já analisado, uma violação de dados pessoais é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Em sede de violação de dados pessoais, o Regulamento Geral de Proteção de Dados prevê diversas disposições que analisaremos brevemente, sem prejuízo de as considerarmos como relevantes para uma eventual ação de responsabilidade civil a intentar por ocorrência de violação de dados.

[81] "*Para além dos custos jurídicos e financeiros, o incumprimento da lei tem ainda outros custos associados que podem ter um impacto negativo muito significativo para as Entidades integrantes do SNS: os custos de imagem e de reputação*.", em manual da PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

1. Responsabilidade do Responsável pelo Tratamento

Neste âmbito e para melhor encadeamento do nosso estudo, considero pertinente atender às disposições e entendimentos existentes, relativamente ao responsável pelo tratamento.

Com efeito, estipula o artigo 4º, n.º7 do RGPD que o responsável pelo tratamento é "*a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro*".

Nestes termos, resulta que é considerado responsável pelo tratamento a pessoa singular ou coletiva que determine as finalidades do tratamento[82] e decida sobre as formas como os dados são tratados, desde a sua recolha, processamento, armazenamento, até ao apagamento. No entendimento da professora Mafalda Miranda Barbosa o responsável pelo tratamento ou *controller "é uma noção dinâmica, que não se deixa aprisionar por determinações abstratas formuladas à priori, antes procurando espelhar o efetivo controlo de facto sobre as finalidades e os meios de tratamento de dados*"[83].

A este propósito e apesar de não nos debruçarmos sobre a responsabilidade do subcontratante no nosso estudo, este é definido nos termos do artigo 4º, n.º8, como "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*", sendo que assumirá o papel de responsável pelo tratamento, no caso de utilizar os dados

[82] Definição de tratamento, nos termos do artigo 4º, n.º 2 do RGPD "*uma operação de tratamento ou um conjunto de operação efetuadas sobre dados pessoais ou sobre conjuntos de 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*".

[83] MIRANDA BARBOSA, Mafalda – "*Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil*" – Revista de Direito Comercial, disponível em www.revistadedireitocomercial.com, 2018;

que lhe foram confiados para a prossecução de determinada finalidade, para outra completamente diferente.

Relativamente ao responsável pelo tratamento, o artigo 28º, n.º1 estipula que "*Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades".* Esta disposição é clara, no sentido de imputar ao responsável pelo tratamento o ónus de garante de cumprimento das disposições do RGPD, relativas ao tratamento de dados pelo qual é responsável. O n.º2 do artigo 24º estipula que "*Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento*.", enquanto que no n.º2 se encontra expresso que a adoção de códigos de conduta[84] ou de procedimento de certificação[85] aprovados conforme o disposto no artigo 42º, podem ser formas de demonstrar o cumprimento das obrigações do responsável pelo tratamento, com a natural relevância que esta disposição acarreta para o nosso estudo.

De acordo com as orientações do GT29[86] acerca do responsável pelo tratamento e do subcontratante, este conceito é autónomo, no sentido de ter que ser interpretado à luz da legislação comunitária em matéria de proteção de dados, bem como funcional, na medida em que delimita a responsabilidade sobre alguém que exerce uma influência de facto (*pode resultar de diferentes circunstâncias jurídicas e/ou factuais: competência prevista expressamente na lei, quando esta nomeia o responsável pelo tratamento ou atribui a tarefa ou o dever de recolher e tratar determinados dados… Na verdade, um organismo que não dispõe de competência legal*

[84] Artigo 40º do RGPD – Disposições sobre Códigos de Conduta
[85] Artigo 42º do RGPD – Disposições sobre Certificação
[86] A este propósito, consultar o Parecer do Grupo de Trabalho do Artigo 29 – Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante» - 2010

nem de influência de facto para determinar o modo de tratamento dos dados pessoais não pode ser considerado o responsável pelo tratamento. [87]) no âmbito do tratamento de dados pessoais que é efetuado.

2. Notificação de uma violação de dados pessoais à autoridade de controlo

No caso de ocorrência de uma violação de dados pessoais, o responsável pelo tratamento, neste caso o Hospital ou Centro Hospitalar, está obrigado a notificar a autoridade de controlo[88] de tal facto, nos termos do previsto no n.º1 do artigo 33º do regulamento[89].

Em regra, esta notificação de violação de dados pessoais terá que ocorrer sem demora injustificada e, nos casos em que tal seja possível, no prazo de 72 horas após o responsável pelo tratamento ter tido conhecimento da mesma, a menos que a violação ocorrida não resulte num risco para os direitos e liberdades do titular dos dados. Em caso de impossibilidade de notificação da violação de dados pessoais, no prazo definido de 72 horas, a notificação terá que ser acompanhada dos motivos do atraso.

Também o subcontratante está obrigado a notificar o responsável pelo tratamento, sem demora injustificada, sempre que tenha conhecimento de uma violação de dados pessoais ocorrida, no âmbito do tratamento de dados que faça por conta do responsável pelo tratamento.

O responsável pelo tratamento deverá documentar as violações de dados pessoais ocorridas, que devem incluir todos os factos com elas relacionadas, os respetivos efeitos e a medida de reparação que tenha sido adotada, com intuito de demostrar perante a autoridade de controlo a verificação de cumprimento das disposições em matéria de notificação de violação de dados pessoais.

---

[87] Ponto IV do Parecer do Grupo de Trabalho do Artigo 29 – Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante» - 2010

[88] Formulário de Notificação de Violação de Dados pessoais disponibilizado pela CNPD https://www.cnpd.pt/DataBreach/?AspxAutoDetectCookieSupport=1

[89] A este propósito, consultar o Parecer do Grupo de Trabalho do Artigo 29 – "*Parecer 03/2014 relativo à notificação da violação de dados pessoais*"

De acordo com as alíneas do n.º3 do artigo 33º do regulamento, a notificação de violação de dados pessoais deverá conter, pelo menos, as seguintes informações:

- *Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;*
- *Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;*
- *Descrever as consequências prováveis da violação de dados pessoais;*
- *Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.*

3. Comunicação de uma violação de dados pessoais ao titular dos dados

Para além do referido no ponto anterior, sempre que se conclua que a violação de dados pessoais é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares[90], o Hospital ou Centro Hospitalar, na qualidade de responsável pelo tratamento é obrigado a comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, nos termos do disposto no

[90] Grupo de Trabalho do Artigo 29 - Parecer 03/2014 relativo à notificação da violação de dados pessoais - Cenários possíveis nos quais a notificação às pessoas em causa não é exigida: "*Embora a avaliação das consequências da violação de dados pessoais deva ser realizada caso a caso, a fim de ter devidamente em conta todos os elementos no decurso da avaliação dos possíveis efeitos adversos sobre os indivíduos, como orientação geral e complemento às isenções descritas na secção anterior, o responsável pelo tratamento de dados pode igualmente considerar que a notificação às pessoas em causa não é exigida em certos casos específicos. Tais casos podem incluir: Uma violação de dados pessoais apenas relativa à confidencialidade, sempre que os dados tenham sido encriptados em segurança com um algoritmo de ponta, que a chave de decifração dos dados não tenha sido posta em causa numa qualquer violação da segurança, e que a mesma tenha sido gerada de modo a que não possa ser determinada, através de meios eletrónicos disponíveis, por qualquer pessoa que não esteja autorizada a aceder-lhe. Com efeito, essas medidas tornam os dados ininteligíveis para qualquer pessoa não autorizada a aceder a eles; Dados, tais como senhas, foram colocados em hash de forma segura e salgados. O valor hash foi calculado com uma função hash de ponta encriptada com chave, a chave utilizada para codificar os dados não foi posta em causa em qualquer violação da segurança, e essa mesma chave foi gerada de modo a que não possa ser determinada, através de meios eletrónicos disponíveis, por qualquer pessoa que não esteja autorizada a aceder a ela.*"

n.º1 do artigo 34º do regulamento, sendo que esta comunicação deve ser efetuada em linguagem clara e simples, descrevendo a natureza da violação dos dados pessoais e fornecendo ao titular dos dados, as informações e medidas previstas no artigo 33º, n.º3, alíneas b), c) e d).

Todavia, a comunicação de violação de dados pessoais ao titular dos dados pode ser afastada, no caso de ser preenchida uma das seguintes condições, previstas nas alíneas a) a c) do nº3 do artigo 34º do regulamento:

- *O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;*
- *O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1 já não é suscetível de se concretizar; ou*
- *Implicar um esforço desproporcionado, em que terá que ser feita uma comunicação pública ou tomada uma medida semelhante, através da qual os titulares dos dados são informados de forma igualmente eficaz.*

4. Direito de Queixa ou Reclamação

Em caso de ocorrência de violação de dados pessoais, os titulares desses dados possuem a faculdade de apresentar reclamação junto da autoridade de controlo, sendo este um meio não contencioso de reportar alguma inconformidade no âmbito do tratamento de dados pessoais. Com efeito, nos termos a alínea f) do n.º1 do artigo 57º do RGPD a autoridade de controlo "*Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80º*", tendo como atribuição ainda *"investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação um prazo razoável, em especial, se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo*".

Ainda a este propósito, atendendo ao considerando 141 "*Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A autoridade de controlo deverá informar o titular dos dados do andamento e do resultado da reclamação num prazo razoável*[91]*. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser comunicadas informações intermédias ao titular dos dados. As autoridades de controlo deverão tomar medidas para facilitar a apresentação de reclamações, nomeadamente fornecendo formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação*".

Estipula ainda o artigo 77º do RGPD que os titulares dos dados têm o direito a apresentar reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o RGPD. Este direito a apresentar reclamação, não coloca em causa outra via de recurso administrativo ou judicial, nos termos do n.º1 do artigo 77º do RGPD.

O direito a apresentação de queixa encontra-se ainda previsto no artigo 33º da Lei 67/98 de 26 de outubro.

[91] Sublinhado nosso.

5. Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante

Nos termos do disposto no n.º1 do artigo 79º do regulamento, está prevista a possibilidade dos titulares dos dados pessoais terem acesso à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do Regulamento Geral de Proteção de Dados, na sequência do tratamento dos seus dados pessoais efetuado em violação do já referido regulamento.

Nos termos do artigo 80º do RGPD, o titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a defesa dos direitos e liberdades do titular dos dados no que respeita à proteção dos seus dados pessoais para, em seu nome, apresentar reclamação, exercer os direitos previstos nos artigos 77º, 78º e 79º, e exercer o direito de receber uma indemnização referido no artigo 82º, se tal estiver previsto no direito do Estado-Membro.

O artigo 82º, n.º1 do regulamento, prevê que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD, tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

Ainda nos termos do n.º2 daquele artigo, qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o RGPD, sendo que no caso do subcontratante, este é responsável pelos danos causados apenas se não tiver cumprido as obrigações decorrentes do RGPD dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

O nível da demonstração de falta de responsabilidade perante o evento que deu origem ao dano, o responsável pelo tratamento ou o subcontratante ficam isentos de responsabilidade, nos termos do n.º2 do artigo 82º do RPGD, no caso de provarem que de modo algum são responsáveis pelo evento que deu origem ao dano.

Ainda assim, sempre que o responsável pelo tratamento tenha pago uma indemnização integral ao titular dos dados que tenha sofrido determinado dano, este tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano, relevando neste ponto a culpa do responsável pelo tratamento no âmbito do dano causado, como defende o professor Almeida Costa "*Se apenas alguns dos solidariamente responsáveis forem culpados, só em relação a estes é admissível o direito de regresso. Os culpados não têm igual direito contra ou não culpados. Entre os culpados, funciona o critério do grau de culpabilidade e dos resultados produzidos*"[92].

Importa de igual forma destacar a disposição do n.º6 do artigo 82º do RGPD, que estabelece que os processos judiciais para exercer o direito de receber uma indemnização são apresentados perante os tribunais competentes, nos termos do direito do Estado-Membro.

Também o artigo 34º da Lei n.º 67/98 de 26 de outubro estabelece que "*Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido*."

Sem prejuízo do já referido em matéria de indemnizações e responsabilidade do responsável pelo tratamento, cumpre efetuar uma breve referência às condições gerais para aplicação de coimas, nos termos do artigo 83º do RGPD, uma vez que poderá ser importante ter em conta as circunstâncias de cada caso, nos termos das alíneas do n.º2 do já referido artigo, nomeadamente considerando o seguinte:

- *A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos;*
- *O caráter intencional ou negligente da infração;*
- *A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares;*

[92] ALMEIDA COSTA, Mário Júlio de – Direito das Obrigações – 12º ed., Almedina, 2018

- *O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º;*
- *Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante;*
- *O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos;*
- *As categorias específicas de dados pessoais afetadas pela infração;*
- *A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram;*
- *O cumprimento das medidas a que se refere o artigo 58.º, n.º 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria;*
- *O cumprimento de códigos de conduta aprovados nos termos do artigo 40.º ou de procedimento de certificação aprovados nos termos do artigo 42.º; e*
- *Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.*

Neste seguimento, cumpre mencionar o disposto no considerando 145[93] *"No que diz respeito a ações intentadas contra o responsável pelo tratamento ou o subcontratante, o requerente pode optar entre intentar a ação nos tribunais do Estado-Membro em que está estabelecido o responsável ou o subcontratante, ou nos tribunais do Estado-Membro de residência do titular dos dados, salvo se o responsável pelo tratamento for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos."*

[93] Regulamento Geral de Proteção de Dados https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

6. Responsabilidade civil do Hospital ou Centro Hospitalar E.P.E., por violação de dados pessoais

Tendo em conta todos os riscos já identificados em matéria de proteção de dados pessoais, nomeadamente atendendo àquela que é a relação complexa entre as entidades prestadoras de cuidados de saúde, os utentes e o direito que os titulares dos dados pessoais têm de exigir indemnização sempre que ocorra uma violação de dados pessoais, no âmbito desta relação Instituição de Saúde/Paciente, cumpre analisar a responsabilidade civil extracontratual do Estado, ao abrigo do disposto na Lei n.º 67/2007 de 31 de dezembro, com as alterações introduzidas pela Lei n.º 31/2008, de 17 de julho, a qual salvaguarda os regimes especiais de responsabilidade civil por danos decorrentes do exercício da função administrativa.

Na opinião da professora Mafalda Miranda Barbosa[94] "*a partir do momento em que um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado – consagradas pelo legislador – no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (responsabilidade pelo outro, ou pelos dados do outro) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da liability (responsabilidade perante o outro)*".

No artigo 22º da CRP, encontra-se estatuído que "*o Estado e as demais entidades públicas são civilmente responsáveis, em forma solidária com os titulares dos seus órgãos, funcionários ou agentes, por ações ou omissões praticadas no exercício das suas funções e por causa desse exercício, de que resulte violação dos direitos, liberdades e garantias ou prejuízo para outrem*", o que na opinião dos professores Gomes Canotilho e Vital Moreira significa que aquele artigo *"não transporta apenas uma lógica indemnizatória-ressarcitória decalcada da responsabilidade do direito civil*"[95], mas também a garantia de um princípio basilar e a proteção de um direito

[94] MIRANDA BARBOSA, Mafalda – "*Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil*" – Revista de Direito Comercial, disponível em www.revistadedireitocomercial.com, 2018;
[95] GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada, Volume I*, 4.ª ed., Coimbra, 2007

fundamental a que os danos causados pelo Estado ou pelas entidades públicas sejam devidamente compensados.

No entendimento do professor Marcelo Rebelo de Sousa, "*A responsabilidade civil administrativa é o conjunto de circunstâncias da qual emerge, para a administração e para os seus titulares de órgãos, funcionários ou agentes, a obrigação de indemnização dos prejuízos causados a outrem no exercício da actividade administrativa*".[96] No âmbito da responsabilidade civil administrativa, esta pode ser classificada de três formas: **quanto à imputação do prejuízo**, a responsabilidade pode ser delitual, pelo risco ou por facto ilícito; **quanto à natureza da posição jurídica subjetiva violada**, a responsabilidade pode ser contratual ou extracontratual; **quanto ao ramo do direito pela qual é regulada**, a responsabilidade civil pode ser por ato de gestão pública ou por ato de gestão privada.

A responsabilidade delitual terá sempre que decorrer de uma conduta reprovada pela ordem jurídica, sendo muitas vezes designada de responsabilidade por facto ilícito e culposo, enquanto que a responsabilidade pelo risco decorre de regras objetivas de distribuição de riscos sociais, quando um dano sofrido extravasa da esfera de risco do lesado, devendo ser outra pessoa a responder por esse mesmo dano. Já a responsabilidade civil por facto lícito, opera sempre que exista necessidade de compensar alguém por um sacrifício a que tenha sido sujeito, através de uma conduta juridicamente conforme e em benefício do interesse público.

No âmbito do nosso estudo, atenderemos apenas à responsabilidade civil extracontratual, uma vez que não estaremos a analisar danos resultantes da execução de um contrato, mas sim da "*afetação de outros direitos subjetivos ou interesses legalmente protegidos*"[97]. Neste sentido, iremos analisar também apenas a responsabilidade civil por ato de gestão pública, deixando de parte a responsabilidade por ato de gestão privada, uma vez que não estamos no âmbito da execução de um contrato.

[96]REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008
[97] REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008

Com efeito, tendo em conta que iremos abordar a questão da responsabilidade civil por danos decorrentes do exercício da função administrativa, consideramos pertinente centrar o nosso estudo na análise da responsabilidade extracontratual delitual, não nos debruçando sobre a responsabilidade extracontratual pelo risco nem por facto lícito. Com efeito, a responsabilidade extracontratual delitual pode ser administrativa ou pessoal, na medida em que importa perceber se a responsabilidade recai sobre a pessoa coletiva administrativa e os titulares de órgãos ou agentes, ou se por outro lado, a responsabilidade é estritamente dos titulares de órgãos ou agentes. Para o professor Marcelo Rebelo de Sousa "*O critério relevante é o da imputação: há responsabilidade administrativa pelos prejuízos provocados por actos que sejam imputados a uma pessoa colectiva administrativa (actos funcionais)*"[98].

Para que um ato seja considerado funcional, terá que cumprir os requisitos cumulativos plasmados nos artigos 7º n.º1 e 8º n.2 da Lei n.º67/2007, na medida em que o ato tem que ser praticado por um titular de órgão, funcionário ou agente da pessoa coletiva; tem que ser praticado no exercício das funções do titular de órgão, funcionário ou agente e por causa desse exercício. Quanto ao dever de indemnizar que decorra da responsabilidade civil delitual, poderá recair quer exclusivamente sobre a pessoa coletiva a quem é imputado o facto que gerou o prejuízo, neste caso pelos danos causados ao titular dos dados nos termos do artigo 7º da Lei n.º67/2007, quer também sobre o titular de órgão, funcionário ou agente que tenha praticado o ato, nos termos do artigo 8º da Lei n.º 67/2007.

Haverá lugar a responsabilidade civil delitual da administração, sempre que se verifiquem os seguintes pressupostos cumulativos: o facto voluntário, a ilicitude[99], a culpa, o dano e o nexo de causalidade.

[98] REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008;

[99] Para o professor Marcelo Rebelo de Sousa no caso de "*faltar o pressuposto da ilicitude, pode haver lugar a responsabilidade por facto ilícito ou pelo risco ou a uma pretensão indemnizatória pelo sacrifício de direitos patrimoniais privados; se faltar o pressuposto da culpa pode ter lugar a pretensão à reconstituição da situação actual hipotética ou o enriquecimento sem causa*". REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André –

1. Facto voluntário: Só existirá lugar à responsabilidade civil delitual por danos que resultem de factos humanos que sejam dominàveis pela vontade, quer por ações quer por omissões, nos termos do disposto nos artigos 7º n.º1 e 8º n.ºs 1 e 2 da Lei n.º67/2007. No entendimento do professor Marcelo Rebelo de Sousa " *Para efeitos de responsabilidade civil constituem ações os regulamentos e os atos administrativos, bem como as simples atuações administrativas e os atos reais, incluindo todas as omissões juridicamente relevantes*"[100];

2. Ilicitude: Nos termos dos artigos 7º n.º1 e 8º n.ºs 1 e 2 da Lei n.º67/2007, terá que existir ilicitude, para que se verifique a responsabilidade civil delitual, sendo ilícita qualquer conduta que seja ilegal, no sentido de violar princípios ou regras constitucionais, disposições legais ou regulamentares, ou disposições decorrentes do direito comunitário, ou mesmo quando se violem regras técnicas ou deveres objetivos de cuidado, nos termos do artigo 9º n.º1 da Lei n.º 67/2007[101], ou os parâmetros pelos quais se fixa aquele que deve ser o funcionamento normal do serviço, nos termos do artigo 9º n.º2 da Lei n.º 67/2007. No entendimento do professor Marcelo Rebelo de Sousa "*Existem duas modalidades básicas de ilicitude: a ilicitude por violação de direitos subjetivos e a ilicitude por violação de normas destinadas a proteger interesses*"[102];

3. Culpa: Nos termos dos artigos 7º nº1 e 8º n.ºs 1 e 2 da Lei n.º67/2007, a culpa é outro dos pressupostos da responsabilidade civil delitual, existindo duas modalidades de culpa: o dolo e a negligência. Nestes termos, existe dolo quando o agente atuou com intenção de provocar o dano, através do dolo direto, dolo necessário ou dolo eventual, existindo negligência quando o agente violou, de forma consciente ou inconsciente, os deveres de cuidado a que estava obrigado, nos casos

Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III – 1ª ed. – D. Quixote, 2008;

[100]REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008

[101] N.º1 do Artigo 9º da Lei n.º 67/2007 "*Consideram-se ilícitas as acções ou omissões dos titulares de órgãos, funcionários e agentes que violem disposições ou princípios constitucionais, legais ou regulamentares ou infrinjam regras de ordem técnica ou deveres objectivos de cuidado e de que resulte a ofensa de direitos ou interesses legalmente protegidos*"

[102]REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008

"*em que o autor prevê a produção do facto ilícito como possível, mas por leviandade, precipitação, desleixo ou incúria crê na sua não verificação, e só por isso não toma as providências necessárias para o evitar*"[103].

Nos termos do disposto no n.º1 do artigo 10º da Lei n.º 67/2007, "*A culpa dos titulares de órgãos, funcionários e agentes deve ser apreciada pela diligência e aptidão que seja razoável exigir, em função das circunstâncias de cada caso, de um titular de órgão, funcionário ou agente zeloso e cumpridor*" sendo que na opinião de João Caupers "*A culpa decorre de um comportamento adoptado com diligência ou aptidão inferiores àquelas que fosse razoável exigir, no caso, a um titular de órgão administrativo, funcionário ou agente zeloso e cumpridor, com base nos princípios e regras jurídicas relevantes*"[104]. De acordo com o disposto nos n.ºs 2 e 3 "*Sem prejuízo da demonstração de dolo ou culpa grave, presume-se a existência de culpa leve na prática de actos jurídicos ilícitos*" bem como "*por aplicação dos princípios gerais da responsabilidade civil, sempre que tenha havido incumprimento de deveres de vigilância*"[105], o que no entendimento de João Caupers significa que "a *culpa leve, menos séria, não está definida na lei, ocorrendo quando o autor da conduta ilícita haja actuado com diligência e zelo inferiores, mas não manifestamente inferiores, àqueles a que se encontrava obrigado. Note-se que a lei, a fim de facilitar a responsabilização, estabelece uma presunção, com base na qual a autoria de um acto jurídico ilícito ou o incumprimento de deveres de vigilância faz presumir a culpa leve*"[106];

4. Dano: Para que se verifique responsabilidade civil administrativa, tem necessariamente que ocorrer um dano, neste caso para o titular dos dados pessoais.

---

[103] ANTUNES VARELA, João – *Das Obrigações em Geral* – Coimbra, Almedina, 2000;
[104] CAUPERS, João - *A Responsabilidade do Estado e Outros Entes Públicos* – Faculdade de Direito da Universidade Nova de Lisboa
[105] OLIVEIRA, Heloísa - Jurisprudência Comunitária e Regime Jurídico da Responsabilidade Extracontratual do Estado e demais Entidades Públicas - Influência, omissão e desconformidade "*O artigo 10.º, n.º 3, do RJRCEE prevê uma presunção de culpa leve na prática de actos jurídicos ilícitos, sob a clara influência da jurisprudência comunitária, que determina a não imposição de condições que dificultem excessivamente ou tornem impossível a obtenção de ressarcimento por violação de direito comunitário, como é o caso do ónus da prova relativamente á culpa*".
[106] CAUPERS, João - *A Responsabilidade do Estado e Outros Entes Públicos* – Faculdade de Direito da Universidade Nova de Lisboa

Para este efeito, podem existir os seguintes tipos de dano: *danos emergentes e lucros cessantes*; *danos presentes e danos futuros*; *danos patrimoniais e danos morais*;

5. Nexo de Causalidade: De forma a operar a responsabilidade civil, é sempre necessário que o resultado de determinada conduta resultante em dano para o titular dos dados, seja imputado ao facto voluntário praticado, nos termos dos artigos 7º, n.º1 e 8º, n.º1 da Lei n.º67/2007. Para este efeito, mencionaremos a explicação do professor Marcelo Rebelo de Sousa acerca da Teoria da Causalidade Adequada[107] "*um dano é imputado a um facto voluntário quando, perante a prática desse, fosse previsível, em condições de normalidade social, a produção do primeiro; em caso de omissão, existe nexo de causalidade quando tenha sido omitida a ação que, em condições de normalidade social, teria previsivelmente permitido impedir a produção do dano*", probabilidade aferida através de juízo de prognose póstuma[108].

Sobre a responsabilidade do responsável pelo tratamento, o considerando 146 do RGPD[109] estipula o seguinte, com especial importância para a nossa análise:

"O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento... Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser

[107]REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008;
[108] Juízo de prognose póstuma é um "*Juízo virtual de prognose formulado após a ocorrência do facto voluntário e do resultado*" REBELO DE SOUSA, Marcelo e outro – *Responsabilidade Civil Administrativa* – 1ª ed. – D. Quixote, 2008
[109] Regulamento Geral de Proteção de Dados (UE) 679/2016

repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento"[110]*.*

Como exemplo daquilo que considero, no âmbito de uma violação de dados pessoais, uma ação ou omissão[111] ilícita, cometida com culpa leve[112] por parte de um funcionário ou agente de um Hospital ou Centro Hospitalar, está um caso em que um funcionário do serviço de Gestão de Doentes, no âmbito do seu desempenho normal de funções, deixa uma folha com uma listagem de doentes para consultas de oncologia em cima da sua secretária, não tendo observado, nesse âmbito o dever de cuidado a que estava obrigado e que por mero caso de estudo, essa lista é divulgada publicamente numa rede social, por parte de terceiro que dela se tenha apoderado. Naturalmente que estamos perante um caso de culpa leve por parte do funcionário do Hospital, que inadvertidamente deixou a folha com a lista com dados especiais em cima da secretária, ausentando-se por momentos, o que terá sido suficiente para que a mesma tivesse sido desviada e posteriormente divulgada por terceiro. Esta ação pode ter causado dano para um dos doentes cujo nome constava da lista, que não queria essa informação divulgada, tendo esse utente, enquanto titular dos dados pessoais em saúde divulgados sem autorização e contra a sua vontade, o direito a ser indemnizado.

Sobre o funcionamento anormal do serviço, estipula o n.º4 do artigo 7º que existe funcionamento anormal do serviço quando, atendendo às circunstâncias e a padrões

---

110 Sublinhado nosso.

111 "*A omissão, como pura atitude negativa, não pode gerar física ou materialmente o dano sofrido pelo lesado; mas entende-se que a omissão é causa do dano, sempre que haja o dever jurídico especial de praticar um acto que, seguramente ou muito provavelmente, teria impedido a consumação desse dano*." ANTUNES VARELA, João – *Das Obrigações em Geral* – Coimbra, Almedina, 2000;

112 Artigo 10º, n.º3 "*Para além dos demais casos previstos na lei, também se presume a culpa leve, por aplicação dos princípios gerais da responsabilidade civil, sempre que tenha havido incumprimento de deveres de vigilância*."

médios de resultado, fosse razoavelmente exigível ao serviço uma atuação suscetível de evitar os danos produzidos. Para o professor Marcelo Rebelo de Sousa "*existem situações em que, apesar de ser objetivamente comprovável que um determinado dano se produziu em virtude da má organização ou do mau funcionamento de um serviço público, não é possível identificar o autor ou os autores dos factos que lhes deram origem… Aplicando estritamente os pressupostos da responsabilidade civil, teria que concluir-se não ser possível a sua efetivação prática, na medida em que, desconhecendo-se o autor do facto a quem respeitam as circunstâncias subjetivas relevantes, não seria possível formular os juízos de dolo ou negligência dos quais depende o preenchimento do pressuposto culpa da responsabilidade civil… Tal solução… contraria os fundamentos da responsabilidade delitual, motivo pelo qual se admite, neste caso, a responsabilização da pessoa coletiva a que pertença o serviço em causa sem necessidade de apuramento da culpa individual*"[113], sendo que no entendimento do professor Fernandes Cadilha, a "*Culpa do Serviço*" contempla "*a culpa colectiva, atribuível a um deficiente funcionamento do serviço, e a culpa anónima, resultante de um concreto comportamento de um agente cuja autoria não seja possível determinar*"[114].

Um exemplo de violação de dados por funcionamento anormal do serviço, poderá ser um caso em que o arquivo físico onde constam os processos clínicos ser acedido por um agente externo ao hospital, sem autorização para tal e sem ser possível aferir qual o trabalhador afeto ao arquivo que deveria ter tomado as diligências necessárias para impedir esse mesmo acesso, não sendo assim possível atribuir aquela falha de serviço a um trabalhador em concreto.

No que diz respeito à responsabilidade solidária em caso de dolo ou culpa grave, estabelece o n.º1 do artigo 8º da Lei n.º 67/2007, que os titulares de órgãos, funcionários e agentes são responsáveis pelos danos que resultem de ações ou omissões ilícitas, por eles cometidas com dolo ou com diligência e zelo

[113] REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008
[114]FERNANDES CADILHA, Carlos Alberto – "*Regime da responsabilidade civil extracontratual do estado e demais entidades púbicas, anotado*"- 2º ed. – Coimbra Editora, 2011

manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo.

Neste âmbito, consideram-se ilícitas, nos termos do n.º1 do artigo 9º da Lei n.º67/2007 as ações ou omissões dos titulares de órgãos, funcionários e agentes que violem disposições ou princípios constitucionais, legais ou regulamentares ou infrinjam regras de ordem técnica ou deveres objetivos de cuidado e de que resulte a ofensa de direitos ou interesses legalmente protegidos, existindo igualmente ilicitude quando a ofensa de direitos ou interesses legalmente protegidos resulte do funcionamento anormal do serviço, segundo o disposto no n.º 3 do artigo 7.º.

Na esfera da culpa dos titulares de órgãos, funcionários e agentes, esta deve ser apreciada pela diligência e aptidão que seja razoável exigir, em função das circunstâncias de cada caso, de um titular de órgão, funcionário ou agente zeloso e cumpridor, nos termos do n.º1 do artigo 10º da Lei n.º 67/2007. A este propósito cumpre atentar na consideração de Antunes Varela, na medida em que refere que "*a culpa exprime um juízo de reprovabilidade pessoal da conduta do agente: o lesante, em face das circunstâncias específicas do caso, devia e podia ter agido de outro modo*.[115]"

Neste âmbito, considero pertinente exemplificar aquilo que para mim será um caso de ação ilícita, cometida pelos membros ou por membro do Conselho de Administração de hospital ou centro hospitalar, com diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo. Assim, o exemplo prende-se com o de um pedido de acesso à informação clínica dirigido à Direção Clínica de um Hospital, efetuado por uma seguradora no âmbito de um seguro de saúde de um utente que, no momento, tem uma doença degenerativa e necessita de cuidados de saúde particularmente dispendiosos e a ministrar em instituição privada de saúde, prestação de cuidados essa abrangida pelo âmbito do contrato de seguro com essa mesma seguradora. Com efeito, acontece que o pedido de acesso à informação clínica é realizado, com o argumento

[115] ANTUNES VARELA, João – *Das Obrigações em Geral* – Coimbra, Almedina, 2000;

de licitude do acesso baseado em cláusula de consentimento para tratamento de dados pessoais em saúde, inserida no âmbito do contrato de seguro, em cláusulas gerais. Este pedido de acesso à informação clínica em particular, é remetido para parecer do Encarregado de Proteção de Dados do Hospital ou Centro Hospitalar, que analisa o pedido e que dá parecer de acesso negativo, por considerar que o consentimento apresentado pela seguradora não é suficientemente expresso, precisamente por existir uma cláusula geral sobre acesso a dados. (a este propósito, devemos atender também ao disposto no artigo 12º, 15º e 16º do Decreto-Lei n.º 446/98, de 25 de outubro que determinam que são proibidas as cláusulas contratuais contrárias à boa fé[116], ponderando-se neste âmbito em especial o seguinte: "*A confiança suscitada, nas partes, pelo sentido global das cláusulas contratuais em causa, pelo processo de formação do contrato singular celebrado, pelo teor deste e ainda por quaisquer outros elementos atendíveis; o objectivo que as partes visam atingir negocialmente, procurando-se a sua efectivação à luz do tipo de contrato utilizado*"[117]). Note-se que neste caso de estudo, o utente titular dos dados não pretende que a informação seja cedida à seguradora, uma vez que considera que tem o direito ao pagamento das despesas relativas a cuidados de saúde e, portanto, não tem interesse em levantar essa informação e apresentá-la ele próprio à seguradora. Neste ponto, considero ainda relevante a análise da Deliberação n.º 51/2001, de 3 de julho de 2001[118], emanada pela Comissão Nacional de Proteção de Dados, nomeadamente atendendo ao ponto VIII, acerca do acesso das companhias de seguro no contexto da morte dos titulares de seguros de vida, analisando precisamente a abordagem realizada ao consentimento contido nas cláusulas gerais, que reveste a mesma importância para o caso em apreço: "*É no momento da celebração do contrato que a seguradora tem que calcular o risco e, por isso, fazer as*

[116] A este propósito, consultar as seguintes sentenças, nos processos infra identificados: Processo n.º 2188/09.6TJLSB do 5º Juízo, 3ª secção dos Juízos Cíveis de Lisboa, proferida a 31 de Dezembro de 2010,
Sentença Processo n.º 2393/09.5YXLSB do 7º Juízo, 3ª Secção dos Juízos Cíveis de Lisboa, proferida a 27 de Janeiro de 2011
Sentença Processo n.º 1810/09.9TJLSB, Juízos Cíveis de Lisboa, proferida a 10 de julho de 2012
[117] Artigo 16º do Decreto-Lei n.º 446/98, de 25 de outubro
[118] Deliberação n.º 51/2001 da CNPD https://www.cnpd.pt/bin/orientacoes/DEL51-2001-ACESSO-DADOS-SAUDE.pdf

diligências sobre o estado de saúde do segurado. Seria de grande interesse para ela, no momento da celebração do contrato, poder dispor da informação que lhe permitisse delimitar o grau de risco. Para o efeito, ou obtém o consentimento ou realiza, também com o seu consentimento, exames ao segurado… Ninguém coloca em causa que, em vida do cidadão, o acesso à informação de saúde em poder da Administração para fins de "instrução de contrato de seguro" só será admissível se for autorizado pelo titular. Estamos perante "situações privadas pactuadas" decorrentes de contrato bilateral alheio à Administração, obrigada a um dever de confidencialidade e de "confidência necessária", e em que domina a autonomia da vontade… A revelação dos dados de saúde viola as disposições legais sobre confidencialidade e reserva da intimidade da vida privada acima enunciadas as quais, na sequência do estabelecido no artigo 268.º n.º 2 da CRP, integram os limites resultantes daquela "reserva de lei". A confrontação do artigo 268.º n.º 2 com as referidas disposições da Lei de Bases da Saúde, do DL n.º 16/93 e com a obrigação de confidência a que estão obrigados os profissionais (Código Deontológico) impõe, necessariamente, a proibição quanto ao acesso à informação."

Não obstante o parecer do Encarregado de Proteção de Dados, a Direção Clínica levou o pedido a reunião do Conselho de Administração, que deliberou pelo diferimento do pedido, tendo a companhia de seguros acedido à informação clínica do titular dos dados, o que levou a que no âmbito da relação contratual existente com a seguradora, as despesas inerentes aos cuidados de saúde ministrados ao utente não tenham sido pagas, tendo causado ao titular dos dados um dano, uma vez que a seguradora considerou que o titular dos dados no momento da celebração do contrato não terá agido de boa-fé, omitindo questões importantes relativas à sua saúde.

Neste âmbito, estabelece o n.º2 do artigo 8º que o Estado e as demais pessoas coletivas de direito público são responsáveis de forma solidária com os respetivos titulares de órgãos, funcionários e agentes, se as ações ou omissões referidas no n.º1 tiverem sido cometidas por estes no exercício das suas funções e por causa desse exercício. Importa ainda referir que nos casos em que haja lugar ao pagamento de indemnização por parte da pessoa coletiva de direito público, esta goza de direito de regresso contra os titulares dos órgãos, funcionários ou agentes responsáveis.

O artigo 3º da Lei n.º 67/2007 de 31 de dezembro, estabelece no n.º1 que quem esteja obrigado a reparar um dano, segundo o disposto naquele diploma, deve reconstituir a situação que existiria se não se tivesse verificado o evento que obriga à reparação sendo, nos termos do n.º2, a indemnização fixada em dinheiro quando a reconstituição natural não seja possível, não repare integralmente os danos ou seja excessivamente onerosa.

Com efeito e no âmbito do caso que analisamos a título de exemplo, teria o lesado, neste caso o titular dos dados indevidamente divulgados à companhia de seguros por culpa da administração do Hospital ou Centro Hospitalar, o direito à indemnização, nomeadamente a que viesse a compensar o mesmo pelas despesas hospitalares que não foram cobertas no âmbito do contrato de seguro.

Por fim, estabelece o n.º6 da Lei n.º 67/2007 que o exercício do direito de regresso, nos casos em que se encontra previsto na lei é obrigatório, sem prejuízo do procedimento disciplinar a que haja lugar.

Identificado que está o risco da ocorrência de ações de responsabilidade civil extracontratual dirigidas aos Hospitais, aos seu órgãos, funcionários e agentes no campo dos dados pessoais relativos à saúde, tratados no âmbito da relação existente entre os utentes e aquelas instituições cumpre, no presente estudo, apresentar uma solução integrada, que permita mitigar ao máximo este risco identificado, protegendo quer as instituições, quer os profissionais, quer os próprios titulares dos dados pessoais.

Capítulo II - Mitigação dos riscos de Violação de Dados Pessoais: Responsabilidade Demonstrável das Entidades de Saúde

Estando identificados os riscos em matéria de responsabilidade civil para as administrações dos Hospitais e Centro Hospitalares E.P.E., nomeadamente a possibilidade dos utentes titulares de dados pessoais serem indemnizados nos termos do artigo 82º do RGPD, bem como das disposições da Lei portuguesa relativamente à responsabilidade civil do Estado, cumpre apresentar uma solução para mitigar precisamente os riscos que foram identificados, nomeadamente tendo em conta todos os aspetos ao nível do tratamento de dados pessoais das instituições do SNS.

Assim, a abordagem que pretendo efetuar é a de apresentar uma solução integral, como um modelo de sistema a implementar pelos Hospitais e Centros Hospitalares do Serviço Nacional de Saúde, adaptado à realidade do nosso país e tendo em conta a composição destas instituições, analisada no início do estudo.

O Sistema de Gestão de Dados Pessoais proposto, assenta na importância de demonstrar perante a autoridade nacional de controlo que a instituição cumpre o Regulamento Geral de Proteção de Dados e que tem a preocupação com as políticas de proteção de dados em cumprimento dos princípios de *privacy by design*[119] e de *privacy by default*[120], sem nunca esquecer a necessidade que o sistema de saúde e as

---

[119] **"***Privacy by design: A preocupação do risco de privacidade deve estar presente em todo o processo de conceção ou contratação de um novo produto, serviço ou projeto, através da implementação de procedimentos adequados desde o início, de modo a garantir que o tratamento está em conformidade com o RGPD e protege devidamente os direitos dos titulares dos dados em causa*", em PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

[120] "*Privacy by default: As entidades devem assegurar que são colocados em prática, mecanismos para garantir que, por defeito, apenas a quantidade necessária de dados pessoais é recolhida, utilizada e conservada para cada tarefa, tanto em termos da quantidade de dados recolhidos, como do tempo pelo qual eles são mantidos, nomeadamente cumprindo o princípio da minimização e da transparência e por exemplo, adotando técnicos como a de «pseudonimização»",* em PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

instituições dele integrantes têm de "*considerar os dados pessoais de saúde como um património privado que se encontra ao seu cuidado, tomando como princípio o segredo da informação de saúde registada*", nas palavras de Sérgio Deodato[121].

1. Possíveis violações de dados pessoais nos Hospitais

Antes de prosseguirmos para a proposta de mitigação dos riscos de violação de dados pessoais, considero pertinente realizar um breve apontamento, sobre aquelas que podem ser as situações relativas ao tratamento de dados pessoais nos hospitais e centros hospitalares, que podem colocar a instituição e os próprios profissionais em situação de vulnerabilidade[122]:

1.1 Pedidos de acesso à informação clínica por parte de familiares

Os pedidos de acesso à informação clínica por parte de familiares são frequentes, nomeadamente quando dizem respeito a utentes em situação de debilidade, que não conseguem efetuar eles próprios o pedido. No entanto, todos os pedidos devem seguir o circuito definido para o acesso à informação clínica, de maneira a que se avalie da legitimidade do acesso e da licitude da disponibilização da informação clínica. O simples facto de um requerente se apresentar como familiar de um utente, não significa que possa ter acesso à informação clínica respeitante a esse mesmo utente. A este propósito, sigo a opinião de Sérgio Deodato "*A revelação de dados*

[121] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;

[122] "*Será necessária a identificação das potenciais vulnerabilidades do sistema, bem como uma previsão do impacto que essas falhas de segurança possam causar, de modo a proceder a uma análise e avaliação de riscos correta e realista que conduzam a uma definição eficaz das medidas de segurança que melhor poderão dar resposta às necessidades da Instituição*", em manual da PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

pessoais de saúde perante familiares, como perante outros, necessita ser consentida pelo seu titular"[123].

1.2 Pedidos de acesso à informação clínica por parte de seguradoras

Os pedidos de acesso à informação clínica por parte de seguradoras são frequentes em meio hospitalar, sendo particularmente sensíveis quando digam respeito a pedidos realizados no âmbito de contratos de seguro de vida. Apesar da frequência dos pedidos, a grande maioria não reveste os requisitos de acesso, porquanto o pedido é efetuado com base nas cláusulas constantes no contrato de seguro. Acontece porém que as referências existentes ao acesso a dados clínicos no âmbito deste tipo de contratos, são muitas vezes gerais e abstratas, não cumprindo na minha opinião os requisitos para que a informação clínica seja disponibilizada.

A este respeito, é também esse o entendimento da CNPD[124] *"A revelação dos dados de saúde viola as disposições legais sobre confidencialidade e reserva da intimidade da vida privada acima enunciadas as quais, na sequência do estabelecido no artigo 268.º n.º 2 da CRP, integram os limites resultantes daquela "reserva de lei". A confrontação do artigo 268.º n.º 2 com as referidas disposições da Lei de Bases da Saúde, do DL n.º 16/93 e com a obrigação de confidência a que estão obrigados os profissionais (Código Deontológico) impõe, necessariamente, a proibição quanto ao acesso à informação. Ainda assim, e mesmo que se pretendesse utilizar um juízo de necessidade e de proporcionalidade que deve presidir à harmonização entre os bens jurídicos conflituantes em presença (art. 18.º n.º 3 da CRP), não há razões objectivas que justifiquem um sacrifício da reserva da intimidade da vida privada em detrimento da invocação de um simples e hipotético "interesse" – sistemático (para todos os casos de morte) e não fundamentado em qualquer suspeita ou indício – que decorre da obrigação de cumprir um contrato. O dever de confidencialidade é estabelecido, conforme se referiu, para salvaguarda da privacidade do doente por exigências de*

[123] DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;
[124] Deliberação n.º 51/2001 da CNPD

interesse público e para defesa da confiança que deve presidir a toda a organização do sistema e da prestação de cuidados de saúde. Este interesse público geral não pode ser sacrificado por hipotéticos e, muitas vezes, mal definidos "interesses" privados de um dos contraentes que pretende satisfazer interesses económicos unilaterais, à custa da violação da intimidade da vida privada do outro contraente. Por isso, entende a CNPD que não será de autorizar o acesso das seguradoras à informação clínica de um segurado para efeito de instrução de processo relativo a seguro de vida.".

Neste âmbito, as informações de saúde apenas devem ser facultadas às seguradoras no caso de a autorização de acesso aos dados de saúde ter sido realizada num documento autónomo, ou pelo menos verdadeiramente destacado das restantes cláusulas gerais do contrato de seguro, garantindo que o consentimento do utente dado em vida, tenha sido "*prestado de modo livre, específico e informado e por forma expressa, pelo titular dos dados de saúde, de acordo com o estatuído no n.º2 do artigo 7º e na alínea h) do artigo 3º da LPD*."[125]

1.3 Informação clínica cedida para o exterior, através de telefone

Os pedidos informação por telefone são recorrentes em ambiente hospitalar, quer seja para saber se determinada pessoa se encontra internada no hospital, quer seja para saber se o estado clínico de determinado utente melhorou, ou em que serviço está o conhecido ou o amigo internado. No entanto, os profissionais dos hospitais e centros hospitalares devem abster-se de prestar qualquer tipo de informação clínica por telefone relativamente a determinado utente, a não ser que tenha sido deixado um número de contacto por parte do utente, com o respetivo consentimento recolhido para a prestação de informação. De outra forma, será uma tarefa árdua e infrutífera controlar a informação que é disponibilizada para o exterior, possivelmente com graves prejuízos para os utentes.

[125] Deliberação n.º 970/2016 da CNPD

1.4 Informação clínica a circular em papel dentro do Hospital

Como já mencionamos anteriormente no nosso estudo, os hospitais possuem um vasto leque de documentação impressa que contem informação clínica. Este tipo de informação pode estar presente nos processos clínicos impressos, em guias de requisição de exames[126] em receitas de medicamentos em papel, nos resultados de análises em papel ou resultados de exames impressos. Neste caso, as instituições enquanto responsáveis pelo tratamento, devem adotar todos os mecanismos que considerem possíveis no sentido de mitigar os riscos de violação de dados presentes neste tipo de operações de tratamento[127],. As melhorias podem ir da retificação ou estabelecimento de procedimentos, passando pela alteração de circuitos, até à anonimização[128] ou pseudonimização de determinados dados pessoais.

1.5 *Malware* nos sistemas informáticos do Hospital

Outra das vertentes abordadas no nosso estudo, teve precisamente que ver com a informação clínica contida em suporte informático nos diversos sistemas e aplicações informáticas que tratam informação clínica relativa aos utentes de um hospital ou centro hospitalar. A título de exemplo mencionamos inclusivamente o ataque informático que ocorreu no Hospital da Orta, através do qual os atacantes sequestraram os exames de todos os utentes daquela instituição, pedido um resgate pela libertação da informação clínica.

---

[126]Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais – CNPD – 2004 "*vários serviços dos hospitais requisitam análises clínicas em suporte de papel, muitas vezes circulando internamente sem o mínimo cuidado e permitindo aos funcionários administrativos – que fazem as marcações das análises – conhecer o «diagnóstico possível», o qual vem anotado nas respectivas requisições*".

[127] Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais – CNPD – 2004 "*Em determinadas doenças discriminatórias – v.g. SIDA/HIV, hepatite, doenças do foro sexual ou oncológico – tem-se verificado que o acesso a esta informação por aqueles profissionais suscita algumas objecções por parte dos cidadãos envolvidos, sentindo que estão a ser discriminados em função da forma como são atendidos. Acresce, por outro lado, que o acesso ao diagnóstico por parte daqueles profissionais (funcionários administrativos) não se apresenta como necessário ao desempenho das suas funções*."

[128] Grupo de Trabalho do Artigo 29 – "*Parecer 05/2014 sobre técnicas de anonimização*"

Neste âmbito, devem os responsáveis pelo tratamento e os seus trabalhadores, adotarem medidas que previnam este tipo de intromissão nos sistemas internos das instituições[129]. A este propósito, devem as instituições de saúde consultar o Manual de Boa Práticas para mitigação dos riscos de segurança da informação[130], bem como seguir as orientações do Centro Nacional de Cibersegurança.[131]

1.6 Furto de equipamentos que contenham bases de dados relativos à saúde

Outra das possíveis formas de ocorrência de violação de dados, tem precisamente que ver com o furto de equipamento eletrónicos, como computadores, *tablets* ou telemóveis que possuam informação clínica armazenada, ou mesmo dispositivos físicos de armazenamento de informação clínica eletrónica, como sejam *pens* ou discos rígidos, os quais contenham informação clínica. Desta forma, devem as instituições garantir que este tipo de dispositivos se encontram devidamente protegidos, por forma a evitar que sejam furtados e que a informação clínica que neles possa constar, seja perdida ou indevidamente divulgada e acedida. Os dispositivos devem ainda conter a informação devidamente encriptada, para dificultar o acesso em caso de furto do equipamento.

1.7 Perfis de acesso aos programas informáticos com dados clínicos

[129] Em caso de ocorrência de incidente de segurança, as entidades devem proceder à notificação de incidentes ao Centro Nacional de Cibersegurança, através do seguinte link: https://www.cncs.gov.pt/certpt/notificar-incidente/

[130] Serviços Partilhados do Ministério da Saúde, E.P.E. – "*Manual de Boa Práticas para mitigação dos riscos de segurança da informação*" disponível em: h*ttp://ciberseguranca.spms.min-saude.pt/wp-content/uploads/2018/03/eSIS_Flyer_Seguranca_da_Informacao.pdf*

[131] Centro Nacional de Cibersegurança – "*atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de Infraestruturas Críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático*." Informação disponível em: https://www.cncs.gov.pt/sobre-nos/

A atribuição de perfis de acesso a programas informáticos que contenham informação clínica a vários profissionais do Hospital, por exemplo ao programa informático S Clínico, sem atribuição de níveis de acesso e sem distinção entre a informação que possa ser acedida por cada grupo profissional, pode acarretar problemas para o hospital, enquanto responsável pelo tratamento. Nesse âmbito, as instituições de saúde devem adotar medidas para, por um lado, consigam avaliar que profissionais têm que ter acesso a estas bases de dados e programas informáticos, para o desempenho das suas funções no dia-a-dia. Por outro, mesmo para estes profissionais que têm que aceder a determinado tipo de informação, é importante que sejam instituídos níveis de acesso, para que nem todos os profissionais tenham permissão para aceder a qualquer tipo de informação, sobre qualquer doente. A esse propósito, considero pertinente mencionar as recentes discussões em torno dos acessos ao S Clínico por parte de profissionais não médicos, com acesso a informação clínica dos doentes no Centro Hospitalar Barreiro Montijo, E.P.E., o que levou a que a CNPD e a IGAS dessem início a investigação no *"caso de acesso irregular a dados clínicos no Hospital do Barreiro, que, segundo o bastonário dos Médicos, pode não ser caso único*"[132].

[132] Acesso irregular a dados clínicos no Hospital do Barreiro vai ser investigado: Citando Miguel Guimarães, Bastonário da Ordem dos Médicos em artigo no Jornal Público, "*A Comissão Nacional de Protecção de Dados (CNPD) e a Inspecção-Geral das Actividades em Saúde vão investigar o caso de acesso irregular a dados clínicos no Hospital do Barreiro, que, segundo o bastonário dos Médicos, pode não ser caso único… A CNPD esteve na segunda-feira no Centro Hospitalar do Barreiro e «vai investigar a situação, porque ficou a sensação de que os dados clínicos dos doentes não têm a protecção que deveriam ter». Além de alertar o Ministério Público, o próximo passo é aguardar a «conclusão quer da investigação da CNPD, quer da Inspecção-Geral das Actividades em Saúde»… «Temos aqui uma área que tem de ser investigada de uma forma geral, se calhar não apenas no Hospital do Barreiro, se calhar é mais extenso do que isso e temos que mudar como estão a ser feitas as coisas neste momento*»", disponível em: https://www.publico.pt/2018/07/03/sociedade/noticia/acesso-irregular-a-dados-clinicos-no-hospital-do-barreiro-vai-ser-investigado-1836751

2. Implementação de Sistema de Gestão de Dados Pessoais

Identificados os riscos inerentes ao tratamento de dados pessoais nos hospitais e centros hospitalares E.P.E., e como forma de prevenir eventuais ações de responsabilidade civil por danos causados aos titulares dos dados pessoais, consideramos que a melhor solução para mitigar estes riscos é proceder à implementação de um verdadeiro Sistema de Gestão de Dados Pessoais, devendo as instituições efetuar os passos que se seguem nos pontos seguintes.

2.1 Constituição de equipa afeta à implementação do Sistema de Gestão de Dados

Os recursos internos de uma instituição serão sempre essenciais para a correta implementação do RGPD, razão pela qual considero de extrema importância que as instituições do Serviço Nacional de Saúde constituam equipas multidisciplinares, compostas por profissionais dos diversos serviços com maior impacto no âmbito da Gestão dos Dados Pessoais da instituição e em particular dos dados relativos à saúde dos utentes.

A seguinte referência serve de mero exemplo do que considero ideal implementar, em termos de equipa afeta à implementação do RGPD, sendo que na minha opinião deverá incluir pelo menos, elementos afetos aos seguintes serviços:

- Serviço de Gestão da Qualidade;
- Serviço de Gestão Logística;
- Serviço de Gestão de Recursos Humanos;
- Serviço de Gestão de Doentes;
- Gabinete Jurídico;
- Serviço de Sistemas da Informação.

Naturalmente que integrará também a equipa afeta à implementação do RGPD o Encarregado de Proteção de Dados a designar, apesar do seu papel no seio da equipa não seja o de executor nem de decisor, mas deverá servir como ponto de apoio e de parecer para as decisões a tomar pela equipa e para as medidas a implementar.

Por fim, destacar a importância de incluir neste grupo de trabalho um elemento do órgão máximo de decisão do Hospital ou Centro Hospitalar E.P.E., nomeadamente um representante indicado pelo Conselho de Administração, de entre os seus elementos. Esta questão é premente, dada a necessidade de envolver o órgão máximo decisor da instituição na implementação do Sistema de Gestão de Dados Pessoais, garantido que a gestão de topo acompanha diretamente as questões relacionadas com a proteção de dados, o que irá contribuir para uma maior consciencialização da administração para estes questões, bem como permitirá uma implementação do Sistema de Gestão de Dados Pessoais de uma forma mais eficaz, o que tendencialmente não iria acontecer, no caso da administração de topo não vir a estar envolvida no processo.

2.2 Realização de Diagnóstico e Avaliação do Hospital

Com vista ao correto diagnóstico e avaliação do Hospital ou Centro Hospitalar E.P.E., a equipa afeta à implementação do Sistema de Gestão de Proteção de Dados Pessoais deverá efetuar os seguintes passos:

- Elaboração de uma reunião com a equipa de implementação, para apresentação do RGPD às diferentes direções de Serviço da instituição;
- Mapeamento de todas as operações de tratamento de dados pessoais do hospital;
- Análise dos fundamentos de recolha, finalidades dos tratamentos, prazos de conservação e demais pressupostos para o tratamento de dados;
- Análise dos "Termos e Condições" e "Políticas de Privacidade" do sítio da internet da instituição;
- Análise dos formulários de recolha de dados e forma de obtenção do consentimento do titular dos dados, no caso de o consentimento ser condição de licitude para o tratamento dos dados[133];

[133] Por exemplo, envio de *newsletters* para os utentes, sobre a atividade do hospital, finalidade que não se prende com a prestação de cuidados de saúde.

- Análise dos tratamentos feitos relativamente aos dados pessoais dos colaboradores da instituição;
- Identificação de tratamento de dados considerados "sensíveis", nomeadamente e em particular os dados de saúde;
- Análise do procedimento adotado para o exercício dos direitos dos titulares, nomeadamente do direito ao apagamento, do direito de acesso, etc.;
- Análise dos mecanismos concretamente implementados para prova do cumprimento do RGPD;
- Análise ao cumprimento das restantes obrigações face ao RGPD, nomeadamente obrigação de nomeação de Encarregado de Proteção de Dados e elaboração de Avaliação de Impacto[134] sobre a proteção de dados para determinados tratamentos de dados pessoais;
- Análise das relações existentes com os Subcontratantes e dos contratos que regulam essas relações;
- Análise dos fluxos transfronteiriços de dados;
- Análise do procedimento e processo para responder às violações de dados, por vezes designados por "*Data Breaches*";
- Elaboração de um relatório final contendo:

    - As desconformidades detetadas e identificadas;
    - O grau de risco decorrente das desconformidades detetadas e identificadas;
    - Plano de mitigação dos riscos em matéria de proteção de dados pessoais;

[134] A este propósito, consultar o sítio da internet da Autoridade de Controlo Francesa, bem como a ferramenta disponibilizada por esta entidade para a realização de AIP's- *CNIL releases a free software for PIA – a tool to help data controllers carry out data protection impact assessment*- Disponível em: https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact

2.3 Nomeação do Encarregado de Proteção de Dados

No caso das instituições integrantes do Serviço Nacional de Saúde e em particular os hospitais e centros hospitalares E.P.E., como pessoas coletivas de direito público, sendo considerados organismos públicos para o efeito constante no RGPD, tem obrigatoriamente que ser designado um Encarregado de Proteção de Dados.

Como já vimos anteriormente, este Encarregado de Proteção de Dados pode ser designado internamente, com recurso aos meios de recursos humanos internos da instituição, ou externamente, com recurso a um contrato de prestação de serviços. Ambas as modalidades têm vantagens e desvantagens, sendo certo que uma entidade que recorra a um trabalhador interno, tem a vantagem deste ter à partida um conhecimento superior dos processos internos, em comparação com um Encarregado de Proteção de Dados com um contrato de prestação de serviços. Ainda assim, no caso de a entidade recorrer a esta modalidade de prestação de serviços, a condição de imparcialidade e autonomia relativamente ao desempenho das funções do Encarregado de Proteção de Dados pode à partida estar melhor assegurada, do que no caso de recurso a trabalhador dos quadros da instituição. Apesar de tudo o que foi dito, esta será uma decisão que caberá ao responsável pelo tratamento, que deverá ter em conta a dimensão da instituição, bem como os recursos disponíveis para efetuar a escolha sobre o encarregado de proteção de dados.

O Encarregado de Proteção de Dados deverá ser designado com base nas suas qualidades profissionais, com base nos seus conhecimentos especializados no domínio do direito e no seu conhecimento das práticas de proteção de dados, devendo exercer as suas funções com a autonomia e independência necessárias, sem existência de incompatibilidades com os restantes serviços, como por exemplo a acumulação da função de Encarregado de Proteção de Dados e de Diretor do Serviço de Recursos Humanos, ou do Serviço Financeiro.

2.4 Designação de Responsável do Acesso à Informação

Em paralelo com a figura do Encarregado de Proteção de Dados e com uma função que não deve ser confundida, devendo estar concretamente autonomizada, encontra-se a figura do Responsável do Acesso à Informação.

Nestes termos, o que defendo em relação a esta figura é que se proceda à nomeação de alguém com a função específica de receber, analisar e avaliar os pedidos de acesso à informação clínica, com o seu posterior envio para o profissional da área clínica com a faculdade de aceder à informação (normalmente por ser um pedido de acesso à informação referente a um utente que tenha estado sob a sua responsabilidade).
Em seguida e após a receção da informação por parte do clínico, este profissional terá o papel de remeter a informação devidamente organizada para a Direção Clínica do Hospital ou Centro Hospitalar E.P.E., para ser finalmente remetida para o requerente da informação.
Contudo, é necessário realizar uma nota de que a presente figura não se encontra prevista nem na lei de proteção de dados portuguesa, nem tão pouco nos estatutos dos Hospitais e Centros Hospitalares E.P.E., sendo si uma adaptação já existente em alguns Hospitais do nosso país, da figura do responsável do acesso, prevista na Lei.º 26/2016, de 22 de agosto, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro, nomeadamente no artigo 9º, prevendo que "*cada órgão ou entidade referida no n.º 1 do artigo 4.º deve designar um responsável pelo cumprimento das disposições da presente lei, a quem compete nomeadamente organizar e promover as obrigações de divulgação ativa de informação a que está vinculado o órgão ou a entidade, acompanhar a tramitação dos pedidos de acesso e reutilização e estabelecer a articulação necessária ao exercício das competências da Comissão de Acesso aos Documentos Administrativos, doravante designada por CADA*."
Note-se que nos termos do n.º3 do artigo 1º "*o acesso a informação e a documentos nominativos, nomeadamente quando incluam dados de saúde, produzidos ou detidos pelos órgãos ou entidades referidos no artigo 4.º, quando efetuado pelo titular dos*

dados, por terceiro autorizado pelo titular ou por quem demonstre ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido na informação, rege-se pela presente lei, sem prejuízo do regime legal de proteção de dados pessoais.", valendo ainda para o efeito o disposto no artigo 7º deste diploma, relativo ao acesso e comunicação de dados de saúde "o *acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico se o titular da informação o solicitar, com respeito pelo disposto na Lei n.º 12/2005, de 26 de janeiro*[135]."

A designação do Responsável pelo Acesso à Informação será necessariamente uma vantagem para os Hospitais e Centros Hospitalares E.P.E., na medida em que, na prática, a sua existência é materializada por um profissional permanentemente dedicado à questão do acesso à informação clínica, com experiência para filtrar todos os pedidos de acesso à informação que cheguem à instituição, diminuindo desta forma o risco de existência de uma tomada de decisão ao nível do acesso à informação, desconforme com a lei de proteção de dados.

2.5 Planeamento da implementação e execução

Não obstante a fase de planeamento da implementação e execução do Sistema de Gestão de Dados Pessoais diferir de instituição para instituição, nomeadamente tendo em conta o resultado da avaliação e diagnóstico inicial, elaborado pela equipa de implementação do sistema, serão necessários implementar ou adaptar os seguintes passos e mecanismos:

- Realização de Ações de formação profissional ao nível do Regulamento Geral de Proteção de Dados, com abrangência a todos os colaboradores da instituição de saúde, incluindo pessoal da área assistencial[136] e do atendimento ao público;

[135] Lei n.º 12/2005, de 26 de janeiro que define o conceito de informação de saúde e de informação genética, a circulação de informação e a intervenção sobre o genoma humano no sistema de saúde, bem como as regras para a colheita e conservação de produtos biológicos para efeitos de testes genéticos ou de investigação.

[136] Sensibilizar, por exemplo, os profissionais da área médica que apenas será possível aceder ao processo clínico dentro da instituição. Nesse sentido, é o entendimento da CNPD "*deve ser impossibilitado o acesso à informação clínica por parte dos utilizadores (médicos ou enfermeiros) através de postos de trabalho externos ao Hospital. Sendo o acesso ao dossier clínico justificado no âmbito do diagnóstico ou prestação de cuidados de saúde, não deverá ser*

- Adaptação dos contratos dos colaboradores da instituição que lidam diretamente com os dados pessoais, com inclusão de cláusulas de confidencialidade nesses mesmos contratos, obrigando os profissionais ao reforço do sigilo profissional, em matéria de tratamento de dados pessoais;

- Adaptação dos fundamentos de recolha, finalidades dos tratamentos, prazos de conservação e demais pressupostos para o tratamento de dados pessoais;

- Alteração aos "*Termos e Condições*" e às "*Políticas de Privacidade*" do sítio da internet da instituição;

- Elaboração de alterações aos contratos com os Subcontratantes, nomeadamente e com particular enfoque nos prestadores de serviços que tratem dados relativos à saúde dos utentes, por conta do hospital ou centro hospitalar;

- Elaboração de alterações aos contratos onde o hospital ou centro hospitalar é Subcontratante, no caso de existirem essas situações;

- Elaboração de um procedimento adequado a responder aos pedidos dos titulares dos dados, nomeadamente respeitante a pedidos de acesso à informação clínica, direito de acesso a dados, direito ao apagamento, direito à limitação do tratamento, etc.);

- Elaboração de mecanismo e procedimento interno para resposta a violações de dados (*Data Breaches*);

- Implementação de Regulamento Interno relativo à Gestão de Dados Pessoais;

---

permitidos aos utilizadores o acesso directo através de terminais colocados no exterior do Hospital", em Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais – CNPD – 2004.

- Elaboração de procedimentos internos adequados, que instituam as formas de tratamento dos terceiros perante situações de tratamento de dados pessoais, por conta do responsável pelo tratamento;

- Implementação de alterações na arquitetura informática, com vista à segurança dos dados pessoais armazenados nos sistemas informáticos e bases de dados da instituição[137];

- Implementação de mecanismos adequados a garantir a segurança dos dados considerados de categorias especiais, nomeadamente os dados relativos à saúde de uma pessoa singular;

2.6 Governo do Sistema de Gestão de Dados Pessoais

Após a fase de planeamento e de execução da implementação do Sistema de Gestão de Dados Pessoais e numa fase em que este sistema se encontra em plena aplicação, garantindo que o hospital ou centro hospitalar E.P.E. cumpre em absoluto com as disposições em matéria de proteção de dados, nomeadamente as constantes na Lei portuguesa e bem assim, garantindo o cumprimento do RGPD, é necessário garantir o adequado acompanhamento e direção do sistema de gestão de dados pessoais implementado na instituição. Nesse âmbito, será necessário que a equipa afeta à implementação do RGPD continue a reunir periodicamente, no sentido de identificar os pontos críticos que possam eventualmente vir surgindo, em matéria de proteção de dados pessoais.

Mais, será necessário que o responsável pelo tratamento, em articulação com o Encarregado de Proteção de Dados, promova as necessárias diligências de

[137] "*Deve ser assegurada a implementação de medidas destinadas a impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança, assim como a separação lógica entre dados de saúde e dados administrativos*", em manual da PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em: http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

auditoria[138] e de fiscalização internas, no sentido de avaliar os procedimentos instituídos em matéria de proteção de dados pessoais e em particular perceber se a instituição está efetivamente a cumprir com aquilo a que se obrigou.

Assim, será sempre necessário garantir nomeadamente o seguinte:

- Que os dados recolhidos apenas são tratados para finalidades determinadas, explícitas e legítimas;
- Que os princípios de *"privacy by design"* e de *"privacy by default",* previstos no artigo 25º do RGPD são devidamente respeitados, na medida em que *"privacy by design"* significa que o "*responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados"*, garantindo que a preocupação pelo risco da privacidade está presente em todo o processo de tratamento de dados, através da implementação de medidas adequadas de proteção desde o início (n.º1 do artigo 25º RGPD) e que *"privacy by default"* significa que o "*responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de*

[138] "*O RGPD prevê... que as Entidades integrantes do SNS adotem as medidas organizativas adequadas para assegurar e poder comprovar que o tratamento de dados é realizado em conformidade com as regras de proteção de dados pessoais. Tais medidas podem incluir a realização de auditorias, a elaboração e implementação de políticas e procedimentos internos, a serem veiculados por toda a Organização*", em manual da PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em: http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

pessoas singulares", colocando as entidades em prática as medidas necessárias para garantir que, por defeito, apenas a quantidade de dados são tratados para cada tarefa, cumprindo o princípio da minimização e da transparência (n.º2 do artigo 25º RGPD)[139];

- Garantir que o circuito de prestação de informação aos titulares dos dados está devidamente estabelecido, nomeadamente existindo uma adequada avaliação da licitude e da legitimidade dos pedidos de acesso à informação e em particular no que diz respeito aos pedidos de acesso à informação clínica;
- Garantir que, para as operações de tratamento em que tal seja necessário, as entidades obtêm o consentimento dos titulares para finalidades de tratamento específicas;
- Garantir que é efetuada uma adequada supervisão dos procedimentos para fazer valer os direitos de acesso, retificação, apagamento, oposição, limitação do tratamento e portabilidade dos dados;
- Avaliar periodicamente as medidas de segurança relativas ao tratamento de dados, em particular as medidas de segurança dos programas e aplicações informáticos[140];
- Garantir que os dados pessoais são conservados apenas pelo período necessário para a finalidade que foram recolhidos[141];

---

[139] A este propósito, releva o teor do considerando 78 do RGPD, nomeadamente o seguinte: "*Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança."*

[140] "*A CNPD considera que só os suportes automatizados dotados das necessárias seguranças – passwords com «perfis de utilizadores» bem definidos, separação lógica entre dados administrativos e de saúde – podem conferir a necessária confidencialidade à informação clínica dos doentes*", em Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais – CNPD – 2004

[141] A este propósito, ter em atenção a Portaria n.º 247/2000 de 8 de Maio, que aprova o regulamento arquivístico para os hospitais e demais serviços do Ministério da Saúde, no que se refere à avaliação, seleção, transferência, incorporação em arquivo definitivo, substituição do suporte e eliminação da documentação

- Garantir um adequado registo das atividades de tratamento de dados;
- Realizar os *"privacy impact assessments"*, ou Avaliações de impacto sobre a proteção de dados, nos termos do artigo 35º do RGPD, nos casos em que tal seja exigido[142];
- Garantir a adequada formação profissional e constante atualização do Encarregado de Proteção de Dados;
- Garantir que o procedimento para notificação de violações de dados e de incidentes de segurança é devidamente seguido;
- Celebrar contratos escritos com todos os prestadores de serviços, incluindo as cláusulas de salvaguarda em matéria de cumprimento do RGPD;
- Pedir, nos casos aplicáveis, consulta prévia à CNPD para os tratamentos de dados, sempre que se conclua através da realização de uma Avaliação de impacto sobre a proteção de dados que exista um elevando risco no tratamento de dados, na ausência de medidas tomadas pelo responsável pelo tratamento para atenuar o risco;
- Adotar cuidados na escolha de prestadores de serviços, que atuaram como entidades subcontratantes, no âmbito de relação contratual com o Hospital ou Centro Hospitalar, na medida em que
- Garantir uma constante consciencialização e sensibilização dos trabalhadores, nomeadamente através de ações periódicas de formação;

---

142 "*Através do PIA, as Entidades integrantes do SNS avaliam e identificam os riscos de determinada operação para a proteção de dados, por forma a, por um lado, antecipar eventuais constrangimentos e, por outro lado, permitir a adoção de medidas que enderecem, minimizem ou eliminem os riscos identificados*", em manual da PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

- Estabelecer níveis de acesso[143] às bases de dados onde se encontram armazenados dados relativos à saúde;
- Garantir uma informatização máxima dos processos clínicos, evitando a conservação e acesso a processos clínicos em papel[144];
- Adotar uma excelente estratégia de comunicação, quer com os trabalhadores do hospital e centro hospitalar, quer com os titulares dos dados, em questões relacionadas com a proteção de dados pessoais;

[143] Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais – CNPD – 2004, "*estabelecimento de «níveis de acesso» em função da natureza da informação tratada, conferindo "medidas de segurança reforçada" e evitando o acesso indevido por pessoas não autorizadas*"

[144]Deliberação n.º 100/2004, de 13 de Julho da CNPD, "*o dossier clínico em suporte de papel não confere as mesmas garantias de confidencialidade que podem ser asseguradas com a informatização do processo clínico*."

Capítulo III - Conclusão

A presente dissertação do mestrado em ciências-jurídico empresariais, teve como objeto a análise da responsabilidade civil dos hospitais E.P.E., bem como dos seus titulares de órgãos, funcionários e agentes. No entanto, este estudo afastou-se da abordagem tradicional em sede de responsabilidade ao nível da atividade normal deste tipo de instituições, analisando sim a responsabilidade na ótica da violação de dados pessoais relativos à saúde, nomeadamente tendo em conta que este tratamento de dados é uma condição essencial para a prestação de cuidados de saúde aos utentes.

Com efeito, pretendi efetuar uma abordagem sobre o direito fundamental à saúde, atendendo à sua natureza pública, através da criação de um Serviço Nacional de Saúde universal e tendencialmente gratuito e o direito à privacidade e à reserva da intimidade da vida privada, também constitucionalmente consagrado. Em seguida, realizei uma análise ao Sistema de Saúde, que é constituído pelo Serviço Nacional de Saúde e por todas as outras entidades públicas que desenvolvem atividades de promoção, prevenção e tratamento na área da saúde, assim como também por todas as entidades privadas e por todos os profissionais livres que acordem com o SNS a prestação de todas ou de algumas daquelas atividades, tendo igualmente sido efetuada uma análise ao Serviço Nacional de Saúde, onde se incluem todas as instituições e serviços oficiais prestadores de cuidados de saúde, que sejam dependentes do Ministério da Saúde.

Naquele encadeamento, e tendo em conta que o presente estudo versou a problemática da responsabilidade civil dos hospitais e centros hospitalares, E.P.E., realizei uma análise ao Decreto-Lei n.º 18/2017 de 10 de fevereiro, que estabelece os princípios e regras aplicáveis às unidades de saúde que integram o Serviço Nacional de Saúde com a natureza de entidade pública empresarial e aprova os seus Estatutos, tendo igualmente sido efetuada uma análise detalhada às competências de cada órgão dos hospitais e centros hospitalares e aquela que é a constituição interna tipo deste género de instituições, para melhor compreensão da dimensão interna e dos serviços existentes.

Em seguida, foi realizada uma abordagem ao tratamento de dados pessoais como fator essencial da prestação de cuidados de saúde, onde se aborda a necessidade premente de tratamento de dados sensíveis ou pertencentes a categorias especiais, no âmbito da prestação de cuidados de saúde das entidades do Serviço Nacional de Saúde, com o objetivo de garantir uma ótima prestação, com base em critérios de segurança clínica e de análise do historial do doente, tendo sido inclusivamente realizada uma análise aos tipos de bases de dados de saúde e de operações de tratamento de dados pessoais em saúde existentes dentro das instituições de saúde do nosso país, quer ao nível informático, quer ao nível de processos manuais.

Foi também realizada uma análise ao regime jurídico da proteção de dados pessoais, tendo nomeadamente sido efetuada uma breve consideração acerca do conteúdo da Lei n.º 67/98 de 26 de outubro, lei essa que versa, ainda[145], sobre a proteção de dados pessoais no nosso país, tendo inclusivamente sido analisada a caracterização de dados pessoais à luz da Lei n.º 67/98 de 26 de outubro, que transpôs para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Tendo ainda em conta a atualidade e a pertinência das questões relativas ao Regulamento Geral de Proteção de Dados n.º 679/2016 UE do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi realizada uma análise detalhada sobre as imposições do regulamento, tendo-se atendido aos conceitos previstos no Regulamento Geral de Proteção de Dados, para melhor compreensão do presente estudo. Ainda neste âmbito e tendo em conta a particularidade e importância da matéria para o nosso estudo, foi realizada uma análise sobre o que são dados pessoais em saúde à luz do RGPD, tendo sido em seguida realizada uma análise sobre o tratamento de dados pessoais em saúde,

[145] É feito este tipo de consideração, tendo em conta a Proposta de Lei n.º 120/XIII, que pretende assegurar a execução, na ordem jurídica interna, do 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, doravante designado abreviadamente por RGPD, prevendo-se que a sua publicação venha revogar a atual lei de proteção de dados em vigor.

nomeadamente sobre a sua proteção e sobre o que legitima o seu tratamento, à luz do regulamento.

Foi também realizada uma abordagem à figura do Encarregado de Proteção de Dados, tendo em conta a obrigatoriedade da sua designação no caso dos hospitais e centros hospitalares E.P.E., tendo sido esta figura encarada como um pilar de responsabilidade interno dentro da instituição de saúde, com um papel muito relevante, quer na defesa da instituição, quer na defesa dos próprios titulares de dados pessoais em saúde. Sobre o Encarregado de Proteção de Dados, ressalta à vista a importância das suas funções ao nível da proteção de dados pessoais e da privacidade, bem como a sua posição dentro da instituição. Ainda em matéria de evidências, foi efetuada uma análise à necessidade de registo das atividades de tratamento de dados dentro dos hospitais e dos centros hospitalares, nomeadamente tendo em conta o impacto que este registo pode trazer para estas instituições, destacando ainda a relevância desta ferramenta para a demonstração de cumprimento das normas relativas à proteção de dados pessoais.

Após a abordagem inicial à realidade dos hospitais e centros hospitalares E.P.E. e do enquadramento realizado ao nível do tratamento de dados pessoais destas instituições, entrou-se na análise à responsabilidade civil dos hospitais por violação de dados pessoais.

Neste âmbito, foi pertinente analisar o tema da notificação de violações de dados pessoais à autoridade nacional de controlo, por um lado, e ao titular dos dados pessoais, por outro lado.

Foi igualmente abordado o direito que o titular dos dados pessoais possui de intentar ação judicial contra um responsável pelo tratamento ou contra uma entidade subcontratante, nos termos do n.º1 do artigo 79º do RGPD, bem como o direito previsto no artigo 82º, n.º1, que prevê que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD, tenha direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

Nesse seguimento, realizámos uma análise à ação de responsabilidade civil contra hospital ou centro hospitalar E.P.E., nos termos da Lei n.º 67/2007 de 31 de dezembro, na sua versão mais recente com as alterações introduzidas pela Lei n.º 31/2008, de 17 de julho, que salvaguarda os regimes especiais de responsabilidade civil por danos decorrentes do exercício da função administrativa, tendo neste âmbito sido abordada a responsabilidade exclusiva do estado e demais pessoas coletivas de direito público, nos casos de danos resultantes de ações ou omissões ilícitas, cometidas com culpa leve, pelos titulares dos seus órgãos, funcionários ou agentes, no exercício da função administrativa e por causa desse exercício.

Foi igualmente analisada a responsabilidade solidária em caso de dolo ou culpa grave, nomeadamente quando se verifiquem danos resultantes de ações ou omissões ilícitas, cometidas por titulares de órgãos, funcionários e agentes com dolo ou com diligência e zelo manifestamente inferiores àqueles a que se encontravam obrigados em razão do cargo.

Para ambos os tipos de responsabilidade foram apresentados exemplos de estudo concretos, tendo-se concluído que os hospitais e centros hospitalares E.P.E. são instituições que, quer pela sua dimensão em termos de trabalhadores e de utentes que recorrem aos seus serviços, quer pela vulnerabilidade dos dados tratados, tendo em conta a especial sensibilidade dos mesmos e as formas de tratamento de dados internamente instituídas, apresentam elevados riscos de ocorrência de violações de dados pessoais, podendo os Hospitais ser diretamente responsabilizados por ocorrências de ações ou omissões que venham a causar dano aos titulares dos dados pessoais, cometidas com culpa leve pelos titulares dos seus órgãos, funcionários ou agentes, no exercício das suas funções. No que diz respeito à responsabilidade solidária em caso de dolo ou culpa grave, foi analisado um caso em que o órgão máximo de administração tomou uma decisão com diligência e zelo manifestamente inferior àquele a que se encontrava obrigado em razão do cargo, não tendo tomado em conta o parecer do Encarregado de Proteção de Dados do Hospital, causando um acesso indevido de informação clínica por parte de uma seguradora, o que causou graves prejuízos ao titular dos dados, com o consequente direito a ser indemnizado na sequência daquela divulgação indevida.

Em sede das conclusões e dos altos riscos identificados de possibilidade de violação de dados pessoais, a ocorrer em hospitais e centros hospitalares E.P.E., e tendo-se concluído que o tratamento de dados pessoais em saúde, efetuado por estas instituições de saúde ultrapassa um tratamento automatizado e informático, devendo considerar-se diversos fatores materiais e humanos, foi proposto um plano para implementação de um Sistema de Gestão de Dados Pessoais.

O principal objetivo da proposta de plano para implementação de Sistema de Gestão de Dados Pessoais, passa precisamente pela necessidade de mitigar os riscos identificados ao nível das possíveis violações de dados pessoais, atendendo aos fatores já identificados.

Assim, é proposto um plano alargado, com vista à articulação interna e envolvimento de vários órgãos e serviços dos hospitais e centros hospitalares, E.P.E., que permita por um lado evitar que as situações como as apresentadas nos exemplos de estudo não se repitam, por um lado, enquanto por outro, permite demonstrar perante os titulares dos dados, as autoridades de controlo e em última análise os tribunais, que o tratamento de dados pessoais efetuado pelas instituições de saúde é realizado com atenção aos princípios e regras em matéria de proteção de dados pessoais e de privacidade, o que levará a que necessariamente os titulares dos dados estejam mais protegidos e que também as instituições e as administrações se consigam defender, em sede de eventuais ações de responsabilidade civil extracontratual.

O plano de ação proposto passa pela constituição de uma equipa afeta à implementação do RGPD, pela realização de diagnóstico e de avaliação do hospital ao nível da conformidade com o RGPD, pela adequada nomeação do Encarregado de Proteção de Dados, pelo planeamento da implementação do sistema e da sua execução, bem como pela necessária atenção aos princípios de bom governo do Sistema de Gestão de Dados Pessoais.

Em suma, o presente estudo conclui que os hospitais e centros hospitalares E.P.E. são das instituições do nosso país com maior vulnerabilidade em matéria de proteção de dados pessoais, existindo um caminho ainda longo a percorrer, com vista ao correto tratamento de dados e de defesa dos titulares dos dados pessoais em saúde. Em paralelo, será impossível de afastar que estas instituições, bem como

as suas administrações, podem estar sujeitas a eventuais ações com vista ao ressarcimento de danos causados pelo tratamento indevido de dados e pela sua divulgação a entidades externas ou terceiros, nomeadamente num momento em que a sociedade portuguesa em geral, desperta para um período de maior conhecimento e de preocupação sobre as matérias relativas à proteção de dados pessoais.

Anexo 1 - Proposta de Regulamento Interno a aprovar nas instituições de Saúde

Preâmbulo

A instituição de saúde, trata dados de saúde de utentes, dados esses considerados como pertencente a categorias especiais de dados, com base no artigo 9º do Regulamento Geral de Proteção de Dados 679/2016 da União Europeia (RGPD).

O RGPD, entrou em vigor a 24 de maio de 2016, tendo aplicação direta e plena em todos os Estados Membros da União Europeia, desde o dia 25 de maio de 2018, tendo introduzido na ordem jurídica europeia novos princípios relativos ao tratamento de dados pessoais, bem como novos direitos dos titulares dos dados pessoais.

O RGPD tem por objeto o estabelecimento de regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O grande objetivo do RGPD é defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

Também a instituição de saúde tem em grande conta a necessidade de proteção dos dados pessoais, quer aqueles que dizem respeito aos seus colaboradores, quer os que dizem respeito aos seus utentes.

No seguimento dessa preocupação e atendendo ao facto de existir alguma dispersão de entendimentos em matéria de proteção de dados pessoais, e no sentido de transmitir alguma orientação aos colaboradores da instituição de saúde, é criado o presente Regulamento Interno sobre o Tratamento de Dados Pessoais na instituição de saúde.

Pretende-se com este Regulamento fixar as regras que devem presidir ao tratamento de dados pessoais na instituição de saúde, nomeadamente o tratamento de dados pessoais relativos aos colaboradores e aos utentes deste Centro Hospitalar.

A instituição de saúde é uma instituição de saúde de referência em Portugal pretendendo, para além de oferecer uma adequada prestação de cuidados de saúde aos seus utentes, ser um símbolo de modernidade e inovação no seio da sociedade.

No desenvolvimento da sua atividade principal, a prestação de cuidados de saúde, a instituição de saúde necessita de proceder ao tratamento de dados relativos à saúde, designadamente os registos de saúde dos utentes, sendo para este efeito o tratamento de dados considerado uma das atividades principais da instituição de saúde.

A instituição de saúde possui um vasto quadro de recursos humanos, sendo que no desenvolvimento das suas funções enquanto empregador, o tratamento de dados pessoais é uma necessidade inultrapassável.

A instituição de saúde cumpre elevados standards de qualidade e conduta, em conformidade com as regras previstas na lei vigente em matéria de proteção de dados e no Regulamento Geral de Proteção de Dados da União Europeia 679/2016, que se traduzam não só no cumprimento da própria lei, mas também no respeito pelos direitos, liberdades e garantias dos seus colaboradores e dos seus utentes.

O presente regulamento interno pretende estabelecer as normas pelas quais os colaboradores da instituição de saúde se devem reger, em matéria de tratamento de dados pessoais, sem prejuízo de outras disposições específicas que regulem esta matéria.

O presente regulamento interno deverá:

- Definir o quadro de finalidades do tratamento de dados pessoais de colaboradores da instituição de saúde;
- Definir o quadro de finalidades do tratamento de dados pessoais de utentes da instituição de saúde;
- Definir, em consequência, o conjunto de dados pessoais de colaboradores e utentes a registar;
- Uniformizar as práticas e procedimentos, a nível interno, no tratamento de dados pessoais de colaboradores e utentes;

- Parametrizar os standards mínimos de qualidade e conduta a ter pelos órgãos da instituição de saúde, seus titulares, funcionários e colaboradores no tratamento dos dados pessoais de membros e prever os respetivos mecanismos de penalização em caso de desrespeito dos mesmos;
- Definir o quadro de direitos, obrigações e competências para os diversos órgãos da instituição de saúde em matéria de tratamento de dados pessoais de colaboradores e utentes;
- Definir, em consequência, os níveis de acesso aos dados pessoais de colaboradores e utentes.

SECÇÃO I

Disposições gerais

Artigo 1.º - Objeto

O presente Regulamento visa definir as regras de tratamento dos dados pessoais tratados pela instituição de saúde, nomeadamente dados pessoais relativos aos seus colaboradores e aos seus utentes, nos termos definidos pela Lei de Proteção de Dados em vigor em Portugal, bem como do Regulamento Geral de Proteção de Dados da União Europeia 679/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Artigo 2.º - Definições

Para efeitos do presente regulamento, entende -se por:

a) «Dados pessoais», toda a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»), sendo identificável 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;

b) «Tratamento de dados pessoais» («tratamento»), é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de 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;

c) «Responsável pelo tratamento», é a instituição de saúde;

d) «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;

e) «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;

f) «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;

g) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

h) «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;

i) «Autoridade de controlo», a Comissão Nacional de Proteção de Dados.

Artigo 3.º - Âmbito de aplicação

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, tratados pela instituição de saúde.

Artigo 4.º - Finalidade do tratamento de dados

1. O tratamento de dados pessoais de colaboradores da instituição de saúde, destina-se a:

a) Exercício das funções normais de entidade empregadora;

d) Manter atualizado o registo disciplinar dos colaboradores;

c) Processamento salarial;

d) Cumprimento de obrigações perante a Segurança Social;

e) Cumprimento de obrigações perante a Autoridade Tributária;

f) Manter contacto regular com os colaboradores, através de correio postal, correio eletrónico, telefone, fax ou qualquer outro meio de comunicação;

g) Enviar publicações da instituição de saúde e qualquer outro tipo de material de divulgação das iniciativas da instituição de saúde ou de interesse para o exercício da prática profissional;

j) Divulgar, a pedido de terceiros e com o consentimento expresso do titular de dados, conteúdos de interesse para o exercício da prática profissional;

k) Elaborar estatísticas sobre a atividade profissional;

o) Credenciar as referências profissionais dos seus membros;

q) Quaisquer outras finalidades legítimas, desde que respeitem a lei, o presente regulamento e os direitos dos titulares.

2. O tratamento de dados pessoais de utentes da instituição de saúde, destina-se a:

a) Prestar cuidados de saúde de forma eficaz e segura;

b) Tratar e reabilitar, em tempo clinicamente adequado, os doentes em condições ótimas de qualidade e humanidade dos serviços prestados;

c) Contatar os utentes para prestação de informação, ou obtenção de informação relevante, no âmbito da prestação de cuidados de saúde;

d) Envio de newsletter com atividade da instituição de saúde, mediante a obtenção de consentimento prévio;

SECÇÃO II

Direitos e deveres dos titulares de dados

Artigo 5.º- Direito de informação

Os titulares de dados têm direito de informação sobre as condições de acesso e de retificação dos seus dados pessoais.

Artigo 6.º - Direito de acesso

1. O titular dos dados tem o direito de obter da instituição de saúde, livremente e sem restrições, informação sobre:

a) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;

b) O conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;

c) A retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na lei ou neste regulamento, nomeadamente devido ao carácter incompleto ou inexato desses dados.

2. O titular dos dados tem ainda o direito de aceder à informação clínica sobre si, que esteja ao cuidado da instituição de saúde.

Artigo 7º - Pedido de Acesso à Informação Clínica

1. O titular dos dados pode a qualquer momento apresentar um pedido de acesso à informação clínica, no sentido de aceder à sua informação clínica constante nas bases de dados da instituição de saúde.

2. O pedido de acesso à informação clínica é oficializado através do preenchimento de impresso próprio, disponível no sítio da internet da instituição de saúde, bem como nos balcões de atendimento ao utente, sendo em todos os casos encaminhado para o Responsável do Acesso à Informação Clínica.

3. Os pedidos de acesso à informação clínica efetuados por terceiros, que não os titulares do acesso à informação, carecem igualmente de preenchimento do impresso de Pedido de Acesso à Informação Clínica, que seguirá o circuito definido para os pedidos de acesso à informação clínica.

Artigo 8.º - Direito de oposição do titular dos dados

O titular dos dados tem o direito de se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para qualquer forma de tratamento, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tal utilização.

Artigo 9º - Direito à Portabilidade dos Dados

O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido à instituição de saúde, nomeadamente dados pessoais relativos à saúde, num formato estruturado, de uso corrente e de leitura automática, bem como o direito de transmitir esses dados a outro responsável pelo tratamento.

SECÇÃO III

Obrigações da Instituição

Artigo 10.º - Segurança do tratamento

1. A instituição de saúde responsabiliza-se por pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

2. A instituição de saúde, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de

segurança técnica e de organização do tratamento a efetuar, e deverá zelar pelo cumprimento dessas medidas.

3. A realização de operações de tratamento em subcontratação será regida por um contrato ou ato jurídico que vincule o subcontratante à instituição de saúde e que estipule, designadamente, que o subcontratante apenas atua mediante instruções da instituição de saúde, incumbindo-lhe igualmente o cumprimento das obrigações referidas no n.º 1.

Artigo 11.º - Medidas especiais de segurança

A instituição de saúde tomará as medidas adequadas para:

a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);

b) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);

c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);

d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);

e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);

f) Garantir que possa verificar-se *à posteriori*, em prazo adequado à natureza do tratamento, quais os dados pessoais introduzidos quando e por quem (controlo da introdução);

g) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

Artigo 12.º - Sigilo profissional

1. A instituição de saúde, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

2. O disposto nos números anteriores não exclui o dever do fornecimento das informações obrigatórias, nos termos legais, exceto quando constem de ficheiros organizados para fins estatísticos.

Artigo 13.º - Publicidade dos dados

1. Os dados pessoais dos colaboradores da instituição de saúde não são de acesso público, salvo o disposto no n.º 2 do artigo anterior.

2. A instituição de saúde pode fornecer dados pessoais de colaboradores e de utentes aos tribunais e demais autoridades públicas com poderes de investigação criminal, se para tal for solicitada por entidade competente.

3. A instituição de saúde pode confirmar se qualquer cidadão figura ou não na sua lista de colaboradores e fornecer o respetivo contacto profissional, no caso de se verificar a legitimidade do pedido da pessoa singular ou coletiva que o requeira.

Artigo 14.º - Responsabilidade civil

1. Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições legais em matéria de proteção de dados pessoais tem o direito de obter da instituição de saúde a reparação pelo prejuízo sofrido.

2. A instituição de saúde pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.

Artigo 15.º – Notificação de Violação de Dados Pessoais à CNPD

1. Sempre que se verifique uma violação de dados pessoais, o colaborador/serviço da instituição de saúde que a identifique, comunica ao Encarregado de Proteção de Dados a ocorrência da mesma, de acordo com o procedimento definido internamente.

2. O Encarregado de Proteção de Dados notifica a Comissão Nacional de Proteção de Dados da violação de dados pessoais, descrevendo a natureza da violação de dados pessoais, incluindo as categorias de dados e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa.

3. A notificação referida no número anterior, deverá conter ainda os contactos do Encarregado de Proteção de Dados, descrever as consequências prováveis da violação de dados pessoais e descrever as medidas adotadas ou propostas pela instituição de saúde para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

SECÇÃO IV

Gestão de dados pessoais

Artigo 16.º - Competências gerais

1. A conservação dos dados pessoais dos colaboradores da instituição de saúde é da responsabilidade de todos os órgãos e serviços, segundo as respetivas competências.

2. A utilização dos dados pessoais dos colaboradores pode ser efetuada por qualquer órgão com legitimidade para o efeito.

3. O bloqueio do acesso aos dados pessoais de colaboradores pode ser deliberado pelos órgãos com legitimidade para o efeito.

4. Os dados pessoais dos colaboradores não são suscetíveis de ser apagados ou destruídos, cabendo à instituição de saúde garantir a sobrevivência dos respetivos suportes digitais.

5. Compete Conselho de Administração da instituição de saúde:

a) Garantir os suportes dos dados pessoais de colaboradores da instituição de saúde;
b) Garantir os suportes dos dados pessoais de utentes da instituição de saúde;
c) Definir as pessoas autorizadas a ter acesso aos dados pessoais dos colaboradores;
d) Definir as pessoas autorizadas a ter acesso aos dados pessoais dos utentes;
e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização;
f) Garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento, quais os dados pessoais introduzidos, quando e por quem;
g) Fazer assegurar o direito de acesso à informação, bem como o exercício do direito de retificação e atualização.

Artigo 17.º - Encarregado de Proteção de Dados

1. A instituição de saúde tem um Encarregado de Proteção de Dados, que nomeia de entre os colaboradores do seu quadro de pessoal.

2. O Encarregado de Proteção de Dados deverá ser escolhido com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções que lhe estão atribuídas.

3. No caso de não existirem no quadro da instituição de saúde, colaboradores que cumpram os requisitos definidos no número anterior, pode ser contrato Encarregado de Proteção de Dados, com base num contrato de prestação de serviços.

4. A instituição de saúde assegura que o encarregado da proteção de dados é envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais.

5. A instituição de saúde apoia o encarregado da proteção de dados no exercício das suas funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

6. O Encarregado de Proteção de Dados não recebe instruções relativamente ao exercício das suas funções, nem pode ser destituído nem penalizado pelo responsável pela instituição de saúde pelo facto de exercer as suas funções.

7. O Encarregado de Proteção de dados informa diretamente a direção ao mais alto nível da instituição de saúde.

8. Os titulares dos dados podem contactar o Encarregado de Proteção de Dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento.

9. O Encarregado de Proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.

Artigo 18.º - Funções do Encarregado de Proteção de Dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha a instituição de saúde ou o subcontratante, bem como os colaboradores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas da instituição de saúde ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos definidos na legislação;
d) Coopera com a autoridade de controlo;
e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º do RGPD e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Artigo 19.º - Responsável do Acesso à Informação Clínica

1. O Responsável do Acesso à Informação Clínica tem como função receber, analisar, processar, encaminhar e responder aos pedidos de acesso à informação clínica da instituição de saúde.

2. O Responsável do Acesso à Informação Clínica é nomeado por deliberação do Conselho de Administração.

3. Compete em especial ao Responsável do Acesso à Informação Clínica:

a) Informar os utentes das suas funções enquanto Responsável do Acesso à Informação Clínica;
b) Informar os interessados sobre o circuito de pedido de acesso à informação clínica;
c) Avaliar da legitimidade e licitude dos pedidos de acesso à informação clínica;
d) Se verificar a ilegitimidade ou ilicitude do pedido, indeferir o mesmo informado o requerente dos motivos;
e) Se o pedido suscitar dúvidas ou carecer de mais informações, é devolvido ao requerente solicitando os dados em falta;
f) Se o pedido for validado favoravelmente, encaminhar o mesmo para um médico relator;
g) Receber a informação do médico relator;
h) Reencaminhar a informação para o secretariado da Direção Clínica, que remete a resposta com informação em anexo para o requerente;

Artigo 20.º - Comissão de Gestão de Dados Pessoais

1. Será constituída uma Comissão de Gestão de Dados Pessoais, composta por um representante do Serviço de Gestão da Qualidade, um representante do Serviço de Gestão de Doentes, um representante do Serviço de Gestão de Recursos Humanos, um representante da Unidade de Apoio Jurídico e um representante do Serviço de Sistemas de Informação, bem como pelo Encarregado de Proteção de Dados da instituição de saúde, a fim de implementar o Regulamento Geral de Proteção de Dados na instituição de saúde e de acompanhar o tratamento de dados pessoais

tratados pela instituição de saúde e propor medidas adequadas à resolução dos problemas emergentes.

2. Compete à Comissão de Gestão de Dados Pessoais:

a) Efetuar, a pedido de qualquer pessoa, a verificação da licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;

b) Apreciar as reclamações e queixas relativas a tratamento de dados pessoais;

c) Apresentar ao Conselho de Administração propostas relativas à organização dos sistemas de dados pessoais;

d) Analisar os relatórios das auditorias em matéria de proteção de dados.

Artigo 21.º - Consulta de dados pessoais

1. A consulta dos dados pessoais dos colaboradores pode ser efetuada pelos próprios, na parte que lhes diga respeito ou por qualquer órgão ou Serviço da instituição de saúde com legitimidade para o efeito.

2. A consulta do nome e endereço eletrónico dos colaboradores da instituição de saúde é uma informação que deve ser disponibilizada publicamente nos termos do artigo 21.º

Artigo 22.º - Comunicação de dados pessoais

1. A comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição dos dados pessoais dos colaboradores está sujeita às restrições referidas no artigo 21.º e pode ser efetuada pelos próprios, na parte que lhes diga respeito e pelo Conselho de Administração.

2. A comunicação de dados pessoais com comparação só é permitida para efeitos estatísticos.

Artigo 23.º - Lista online de contactos dos colaboradores

1. É disponibilizado o acesso interno a uma lista online dos colaboradores da instituição de Saúde, disponível na Intranet, que permita identificar, pelo nome e/ou Serviço, qualquer colaborador.

2. A lista online não pode ser utilizado para gerar listas de endereços com fins comerciais.

3. O abuso sobre a informação contida na lista online será sancionado nos termos disciplinares e legais.

SECÇÃO V

Autoridade de Controlo

Artigo 24.º - Cooperação com a CNPD

1. A instituição de saúde coopera com a CNPD, nos termos da lei e a pedido desta, na prossecução das suas atribuições.

2. A instituição de saúde cumpre ainda as suas obrigações perante a CNPD, nomeadamente as relativas à comunicação de violação de dados pessoais nos termos do artigo 15º do presente regulamento interno e do artigo 33º do RGPD e da realização de Consulta prévia, nos termos do artigo 36º do RGPD.

Artigo 25.º - Apreciação pela CNPD

A instituição de saúde submeterá este regulamento à apreciação da CNPD, a fim de certificar a sua conformidade com as disposições legais vigentes em matéria de proteção de dados pessoais.

SECÇÃO VI

Infrações

Artigo 26.º - Infrações

São passíveis de procedimento criminal, nos termos da lei, os seguintes atos:

a) Fornecer falsas informações ou proceder a modificações de dados não autorizados;

b) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha;

d) Não cumprir obrigações determinadas pela lei ou pela CNPD;

e) Aceder a dados sem a devida autorização;

f) Violar regras técnicas de segurança;

g) Possibilitar indevidamente a terceiros o conhecimento de dados pessoais;

h) Proporcionar ao agente ou a terceiros benefício ou vantagem patrimonial;

i) Apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis.

Artigo 27.º - Responsabilidade Disciplinar

Para além do disposto no artigo anterior, é passível de procedimento disciplinar qualquer comportamento ou ato de colaborador da instituição de saúde que viole as políticas e procedimentos internos relativos à proteção de dados pessoais.

SECÇÃO VII

Disposições finais e transitórias

Artigo 28.º - Disposição transitória

Os dados existentes em ficheiros manuais e eletrónicos anteriores serão conservados unicamente com finalidades de investigação histórica.

Artigo 29.º - Entrada em vigor

O presente Regulamento entra em vigor no dia seguinte ao da sua publicação na Intranet da instituição de saúde.

Anexo 2- Proposta de Política de Privacidade

O HOSPITAL, E.P.E. (adiante designado HOSPITAL) é uma pessoa coletiva de direito público de natureza empresarial, dotada de autonomia administrativa, financeira e patrimonial, pretendendo ser um Centro Hospitalar de referência na prestação de cuidados de saúde, com especialidades diferenciadas, apostando no desenvolvimento de serviços eficientes e inovadores, com uma gestão adequada dos recursos, sempre com o objetivo de atingir a satisfação dos seus utentes.

No desenvolvimento da sua atividade principal, a prestação de cuidados de saúde, o HOSPITAL é também responsável pela recolha, processamento e utilização de dados pessoais dos utentes, sendo para o efeito do presente documento o "*Responsável pelo Tratamento*".

Os dados pessoais tratados pelo HOSPITAL, sendo dados pessoais relativos à saúde de uma pessoa, são pertencentes a categorias especiais de dados, sendo que o seu tratamento respeita determinadas condições, nos termos da Lei de Proteção de Dados em Portugal e do Regulamento Geral de Proteção de Dados 2016/679 UE.

No âmbito da recolha de dados necessária para a prestação de cuidados de saúde no HOSPITAL, tem o titular dos dados o direito a saber as seguintes informações:

Responsável pelo Tratamento:

O responsável pelo tratamento é o HOSPITAL, E.P.E., determinando as finalidades e os meios de tratamento de dados pessoais dos utentes. O contacto do HOSPITAL é o seguinte: geral@hospital.min-saude.pt

Encarregado de Proteção de Dados:

O Encarregado de Proteção de Dados (*Data Protection Officer*) do HOSPITAL é _____, sendo o seu contacto eletrónico o seguinte epd@hospital.min-saude.pt

Dados Pessoais recolhidos e finalidades do tratamento:

- **Dados de contacto -** Com vista a comunicar com o titular dos dados pessoais no âmbito das suas atribuições, nomeadamente a prestação de cuidados de saúde, o HOSPITAL recolhe os dados de contacto (nome, país de origem, endereço de email e número de telefone).
- **Informações clínicas e de saúde -** Com vista à prestação de cuidados de saúde, o HOSPITAL recolhe informações clínicas e de saúde relacionadas com os seus utentes. Estas informações são solicitadas pelo clínico responsável pelo tratamento, que regista essas mesmas informações no processo clínico respetivo.

Utilização de dados pessoais

O HOSPITAL recolhe, processa e utiliza os dados pessoais supra mencionados, exclusivamente no âmbito da prestação de cuidados de saúde.

Destinatários dos Dados

Os dados tratados no âmbito da relação HOSPITAL-paciente são armazenados nos sistemas informáticos internos, ou sistemas informáticos supervisionados pelos Serviços Partilhados do Ministério da Saúde, E.P.E., sendo suscetível o seu acesso, noutras instituições do SNS. Não obstante, o acesso aos dados pessoais constantes nos já referidos programas informáticos, apenas é permitido no âmbito da prestação de cuidados de saúde do titular dos dados.

Prazo de Conservação dos Dados

Os dados pessoais recolhidos, serão conservados durante o tempo em que se mantiver a prestação de cuidados de saúde relativamente ao titular dos dados, bem

como durante o prazo legalmente previsto para conservação de informação arquivada pelos hospitais, consoante o tipo de informação.

Direito de acesso, retificação ou apagamento

O titular dos dados tem o direito de solicitar ao HOSPITAL acessos aos dados pessoais que lhe digam respeito, bem como à sua retificação ou ao seu apagamento, nos termos dos artigos 15º, 16º e 17º do RGPD. Para este efeito e para quaisquer questões adicionais que possa ter relativas à proteção de dados e ao processamento dos seus dados pessoais, o titular dos dados deverá contactar o HOSPITAL através do seguinte enderenço de correio eletrónico: geral@hospital.min-saude.pt

Direito à limitação do tratamento

O titular dos dados tem direito de solicitar ao HOSPITAL a limitação do tratamento de dados, nos termos do artigo 18º do RGPD.

Direito à Portabilidade dos Dados

O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido ao HOSPITAL num formato estruturado, de uso corrente e de leitura automática, bem como o direito a transmitir esses dados a outro responsável pelo tratamento, nos termos previstos no artigo 20º do RGPD.

Direito a apresentar reclamação à Autoridade de Controlo

O titular dos dados toma conhecimento de que é seu direito apresentar reclamação à Comissão Nacional de Proteção de Dados, no âmbito do tratamento dos seus dados pessoais.

Obrigatoriedade de fornecimento de dados

O titular dos dados deverá fornecer os dados pessoais que lhe sejam solicitados no momento da admissão no HOSPITAL, salvo casos de manifesta impossibilidade. Caso o titular dos dados se recuse a disponibilizar alguns dos dados solicitados, o HOSPITAL não se responsabiliza pelo normal encaminhamento do processo do utente dentro do Serviço Nacional de Saúde, incluindo o respetivo endosso de assistência, pese embora em momento algum seja colocado em causa o direito a receber os cuidados de saúde.

Segurança dos dados

Adotámos medidas técnicas e organizacionais adequadas para proteger os seus dados pessoais armazenados nos nossos sistemas de TI contra perda, destruição, acesso não autorizado, alteração ou divulgação.

Anexo 3 – Proposta de Procedimento de Divulgação de Informação Clínica a entidades externas

1. O objetivo do presente procedimento é o de garantir a confidencialidade e a segurança da informação clínica, definindo critérios a considerar na divulgação da informação clínica a entidades externas.

2. O presente procedimento aplica-se a todos os pedidos de acesso à informação clínica efetuados por entidades externas ao Hospital.

3. Neste âmbito, entende-se por entidades externas ao Hospital, entre outras possíveis, as seguintes: o *utente*, *familiares do utente*, *Tribunais*, *órgãos de polícia criminal*, *companhias de seguros*, *subsistemas de saúde*, *juntas médicas*, *advogados*, etc.

4. Os pedidos de acesso à informação clínica são obrigatoriamente dirigidos ao **Diretor Clínico** do Hospital ou ao **Responsável do Acesso à Informação (RAI)**, através de correio eletrónico (rai@hospital-min.saude.pt) ou de impresso próprio disponibilizado no Hospital para o efeito.

5. No caso de o pedido entrar pelo **Diretor Clínico**, o secretariado receciona e regista o pedido, reencaminhando o mesmo para o gabinete do **RAI**, no prazo de 3 dias. Caso o pedido de acesso à informação clínica seja diretamente dirigido ao **RAI**, este procede à avaliação do mesmo.

6. Os pedidos de acesso à informação clínica devem ser bem fundamentados e especificar os motivos pelos quais o pedido é efetuado, bem como qual o tipo de informação requerida.

7. O **RAI** avalia o pedido e procede de uma das seguintes formas, no prazo de 5 dias:

a) Considera que não existe legitimidade e/ou licitude no pedido efetuado e indefere o mesmo, informando o requerente dos motivos de indeferimento;
b) Considera necessário solicitar parecer ao **Encarregado de Proteção de Dados (EPD)**, que avalia e emite parecer positivo ou negativo, quanto ao

acesso à informação clínica «*no caso do parecer ser negativo, procede como descrito em a). No caso do parecer ser positivo, procede como descrito em c)*»;

c) Encaminha o pedido para o Diretor de Serviço da especialidade em que o utente recebeu os cuidados, que elabora relatório clínico, contendo a informação requerida, ou que recolhe os exames ou registos clínicos requeridos;

8. O relatório é elaborado no prazo de 10 dias pelo Diretor do Serviço responsável, ou por médico do Serviço por este designado.

9. O médico que elabora o relatório envia apenas a informação que considere necessária para responder ao pedido do requerente.

10. O relatório clínico ou os exames e registos clínicos, são remetidos para o **RAI**, que reencaminha os mesmos para o **Diretor Clínico**, acompanhados de parecer sobre a legitimidade e licitude do acesso à informação.

11. O reencaminhamento para o **Diretor Clínico** é realizado com recurso a meios informatizados e com as devidas medidas de segurança técnicas, adequadas para garantir a confidencialidade da informação.

12. O **Diretor Clínico** possui de 5 dias para avaliar o teor do relatório clínico, ou os exames e registos clínicos a enviar, bem como o parecer do **RAI** e/ou do **EPD**, no caso de ter sido solicitado, procedendo de uma das seguintes formas:

a) Dá indicação para o secretariado remeter a informação para a entidade requerente, cumprindo todos os requisitos de segurança que estiverem ao seu alcance para garantir a privacidade do titular dos dados;
b) Solicita ao médico que elabora o relatório, a reformulação de determinado aspeto nele constante;

Critérios de Divulgação de Informação Clínica

Os pedidos de acesso à informação clínica são avaliados de acordo com os seguintes critérios e outros, dispostos na Lei de Proteção de Dados Pessoais:

a) **Pedido de acesso à informação clínica realizado por utente;**

Em regra, os pedidos de acesso à informação clínica realizados por utente são deferidos, em cumprimento com o direito de acesso à informação que assiste aos titulares dos dados. No entanto, poderão existir razões em que, exclusivamente por razões clínicas e em proteção do estado de saúde do utente, a informação clínica poderá não ser divulgada.

b) **Pedido de informação relativa a cuidados de saúde para pagamento de faturas por seguradoras e subsistemas de saúde;**

Os dados a comunicar para este efeito, devem ser os estritamente necessários para proceder à faturação e à cobrança dos cuidados de saúde prestados. A comunicação será sempre feita a profissional de saúde obrigado a sigilo ou a outra pessoa igualmente sujeita a sigilo profissional, devendo as seguradoras e os subsistemas indicar qual o profissional responsável por receber a informação enviada.

c) **Solicitações de médicos assistentes, instituições de saúde e seguradoras, tendo em vista a continuidade de prestação de cuidados;**

O relatório a enviar, bem como todos os exames efetuados disponíveis, devem ser enviados ao médico que assegurar a continuidade de cuidados.

d) **Pedidos formulados para elaboração de relatório de reforma e aposentação;**

Estes pedidos devem indicar o médico à ordem de quem deve ser enviada a informação clínica. Os relatórios podem ser efetuados a pedido do interessado, das juntas médicas ou das entidades que concedem reforma por incapacidade.

e) Pedido de documentação a solicitação dos Tribunais;

No âmbito de pedidos de informação clínica efetuados pelos tribunais, é facultada a informação estritamente necessária para corresponder à finalidade para a qual os dados foram requeridos. Nos casos dos pedidos de acesso que não se encontrem devidamente fundamentados e circunscritos a determinada finalidade, os mesmos serão indeferidos.

f) Pedidos de informação clínica de órgãos de polícia criminal;

Os pedidos de acesso à informação clínica por parte de órgãos de polícia criminal são, em regra, indeferidos. Não obstante, em cumprimento do dever geral de cooperação entre as instituições, podem ser fornecidos elementos de identificação dos utentes como o *nome, idade, morada ou o número de identificação civil* ou informações genéricas sobre o estado de saúde dos utentes, como a *morte, gravidade da situação necessidade de internamento ou a existência de lesões visíveis*;

g) Pedidos efetuados por advogados;

Os pedidos de acesso à informação clínica realizados por advogados, apenas podem ser deferidos nos casos em que estes apresentem procuração com poderes especiais para acesso aos dados de saúde de determinado utente.

h) Acesso a dados por familiares de utentes falecidos;

A proteção de dados de utentes falecidos mantém-se após a morte, considerando-se que apenas poderão ser fornecidas informações *post mortem* a pedido de familiar direto ou legítimo herdeiro, nos seguintes casos:

- Relatório de autópsia ou relatório onde conste a causa da morte, a requerimento de familiares ou herdeiros;
- Relatório sobre a situação clínica e os cuidados prestados quando os familiares ou herdeiros invocarem a necessidade, devidamente justificada e fundamentada, de acesso aos dados para intentar processo judicial (contra o hospital, seguradora, etc.). A informação fornecida só pode ser utilizada exclusivamente para a finalidade requerida;

- Relatório clínico, a pedido do médico assistente do familiar do utente falecido, no caso de ser necessário tomar medidas preventivas ou fazer diagnóstico de doença hereditária ou genética;

i) Pedidos de Seguradoras no contexto de morte de titulares de seguros de vida;

Os pedidos de acesso à informação clínica no âmbito de morte do titular de seguro de vida são, por regra, indeferidos. A informação às seguradoras apenas será fornecida no caso de esta evidenciar que o titular dos dados deu, em vida, um consentimento de modo livre, específico e informado e por forma expressa.

Proibição de fornecimento de informação clínica

Todo e qualquer outro pedido de acesso à informação clínica realizado fora do âmbito do circuito definido neste procedimento, deve ser imediatamente indeferido, devendo os requerentes ser devidamente informados da existência de procedimento específico para acesso à informação.

Os profissionais do Hospital devem igualmente abster-se de prestar informação clínica a entidades externas fora do presente circuito, quer seja por telefone, correio eletrónico ou presencialmente, de forma a garantir a proteção dos titulares dos dados pessoais, das instituições de saúde e dos próprios profissionais.

Referências Bibliográficas

ALMEIDA COSTA, Mário Júlio de – *Direito das Obrigações* – 12º ed., Almedina, 2018

ALMENDRA FREITAS PIRES, Lucas de, Dissertação "*Direito à Privacidade no âmbito da sociedade de informação: reflexões em torno da questão nos inícios do século XXI*", Dissertação de mestrado apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do Mestrado Científico, Coimbra, 2014.

ANTUNES VARELA, João – *Das Obrigações em Geral* – Coimbra, Almedina, 2000;

AMADO GOMES, Carla – *Nota breve sobre a tendência de objectivação da responsabilidade civil extracontratual das entidades públicas no regime aprovado pela Lei 67/2007, de 31 de Dezembro* – Responsabilidade Civil dos Estado, Centro de Estudos Judiciários, disponível em:
http://www.cej.mj.pt/cej/recursos/ebooks/civil/Responsabilidade_Civil_Estado.pdf

BAPTISTA MANSO, Luís Duarte e TEODÓSIO OLIVEIRA, Nuno - *Direito das Obrigações, casos práticos resolvidos* – 6ª ed., Quid Juris, 2010;

CALVÃO, Filipa Urbano - *Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina* - 1.ª edição, Universidade Católica, 2018;

CARVALHO, Ana Celeste - *Regime Processual Aplicável no Âmbito do Artigo 8.º, N.º 4, da Lei de Responsabilidade Civil do Estado e Demais Entidades Públicas* , - in Julgar, nº15, 2011, disponível em:
http://julgar.pt/wp-content/uploads/2014/07/10-DEBATER-Regime-processual-de-responsabilidade-civil-do-Estado.pdf

CAUPERS, João - *A Responsabilidade do Estado e Outros Entes Públicos* – Faculdade de Direito da Universidade Nova de Lisboa;

CAUPERS, João, "*Notas Sobre a Lei da Responsabilidade do Estado e Outros Entes Públicos*", disponível em: www.fd.unl.pt/docentes_docs/ma/jc_MA_5351.doc;

CASANOVA, Salazar - *Introdução á temática do dano na responsabilidade civil* - disponível no e-book do CEJ, em:
http://www.cej.mj.pt/cej/recursos/ebooks/civil/O_Dano_Responsabilidade_Civil.pdf

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, "*Deliberação nº 970/2016*", Disponível em *http://www.cnpd.pt;*

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, "*Deliberação nº 51/2001*", Disponível em *http://www.cnpd.pt;*

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, "*Deliberação nº 72/2006*", Disponível em *http://www.cnpd.pt;*

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, "*Parecer 18/2000*", Disponível em *http://www.cnpd.pt;*

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS, "*Parecer n.º442/2015*", Disponível em *http://www.cada.pt/;*

DEODATO, Sérgio – *Proteção dos dados pessoais de Saúde* – Universidade Católica Editora, 2017;

ENTIDADE REGULADORA DA SÁUDE, "*Parecer sobre o acesso a informação de saúde*", disponível em: *https://www.ers.pt/uploads/writer_file/document/1582/Publica__o_Parecer_-_ERS_016_2015.pdf*

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE - *Handbook on European data protection law* – Luxemburgo, Publications office of the European union, 2018;

ESTORNINHO, Maria João e MACIEIRINHA, Tiago – *Direito da Saúde* – Lisboa, Universidade Católica Editora, 2014;

FAZENDEIRO, Ana – *Regulamento Geral de Proteção de Dados* – 2º ed. – Almedina, 2017;

FERNANDES CADILHA, Carlos Alberto – *Regime da responsabilidade civil extracontratual do estado e demais entidades púbicas, anotado* - 2º ed. – Coimbra Editora, 2011;

GOMES CANOTILHO e VITAL MOREIRA, - *Constituição da República Portuguesa Anotada, Volume I* - 4.ª ed., Coimbra, 2007

GUERRA, Amadeu, - *Relatório de Auditoria ao Tratamento de Informação de Saúde nos Hospitais* - CNPD, 2004, disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Orientações sobre os encarregados da proteção de dados (EPD)*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 03/2014 relativo à notificação da violação de dados pessoais*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Documento de Trabalho sobre os Dados Genéticos*", 2004, Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 8/2010 sobre a lei aplicável*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 15/2011 sobre a definição de consentimento*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 06/2012 sobre o projeto de decisão da Comissão relativa às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE relativa à privacidade e às comunicações eletrónicas*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 3/2013 sobre a limitação da finalidade*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 05/2014 sobre técnicas de anonimização*", Disponível em *http://www.cnpd.pt;*

GRUPO DE TRABALHO DO ARTIGO 29 "*Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE*", Disponível em *http://www.cnpd.pt;*

LEITÃO, Alexandra – *Duas questões a propósito da responsabilidade extracontratual por (f)actos ilícitos e culposos praticados no exercício da função administrativa: da responsabilidade civil à responsabilidade pública. Ilicitude e presunção de culpa* - disponível em:
http://www.icjp.pt/sites/default/files/media/artigo-responsabilidade2.pdf

LOUREIRO CUNHA, Luís Filipe - *A Responsabilidade Civil por actos da Administração Pública* - Dissertação de mestrado, disponível em:
http://recil.grupolusofona.pt/bitstream/handle/10437/4953/Luis/prct.20Filipe/prct.20Loureiro/prct.20Cunha.pdf?sequence=1

MAGALHÃES, Filipa Matias e PEREIRA, Maria Leitão - *Regulamento Geral de Proteção de Dados: Manual Prático* - 2.ª edição revista e ampliada, Vida Económica, 2018;

MIRANDA BARBOSA, Mafalda – *Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil* – Revista de Direito Comercial, 2018, disponível em*www.revistadedireitocomercial.com;*

OLIVEIRA, Heloísa - *Jurisprudência Comunitária e Regime Jurídico da Responsabilidade Extracontratual do Estado e demais Entidades Públicas - Influência, omissão e desconformidade* – Instituto de Ciências Jurídico-Políticas, disponível em: *http://www.icjp.pt/sites/default/files/media/645-963.pdf*

PRIVACIDADE DA INFORMAÇÃO NO SETOR DA SAÚDE, Serviços Partilhados do Ministério da Saúde, disponível em:
http://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf

QUADROS, Fausto de "*A Responsabilidade Civil Extracontratual do Estado - Problemas Gerais*", ao Ministério da Justiça, ao Gabinete de Política Legislativa e Planeamento, Lisboa, 2001, disponível em:
http://www.dgpj.mj.pt/sections/informacao-e-eventos/anexos/sections/informacao-e-eventos/anexos/prof-doutor-fausto-de/downloadFile/file/Fq.pdf?nocache=1210675906.12

REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Direito Administrativo Geral, Tomo I* – 5º ed. – D. Quixote, 2014;

REBELO DE SOUSA, Marcelo e SALGADO DE MATOS, André – *Responsabilidade Civil Administrativa, Direito Administrativo Geral, Tomo III* – 1ª ed. – D. Quixote, 2008;

RELATÓRIO 1999 DA CNPD, Disponível em *www.cnpd.pt;*

RELATÓRIO DE DIAGNÓSTICO AO ARQUIVO CLÍNICO, Secretaria-Geral do Ministério da Saúde, 2018;

SÉRVULO CORREIA, José Manuel – As relação jurídicas administrativas de prestação de cuidados de saúde – disponível em:
https://www.icjp.pt/sites/default/files/media/616-923.pdf

SILVA MOREIRA, Lucas – *A responsabilidade civil extracontratual do estado no exercício da função administrativa nos sistemas brasileiro e português* – Dissertação de mestrado apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º ciclo de estudos em Direito, Coimbra, 2014

SILVEIRA, João Tiago - *A Reforma da Responsabilidade Civil Extracontratual do Estado* -, disponível em:
http://joaotiagosilveira.org/mediaRep/jts/files/Responsabilidade_Civil_Extracontratual_-_Revista_Jur__dica_26.pdf

OUTROS LINKS NA INTERNET

https://www.cnpd.pt/bin/rgpd/rgpd.htm

https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

https://ec.europa.eu/info/law/law-topic/data-protection/reform_pt

The Internet and the Global Reach of EU Law:
https://poseidon01.ssrn.com/delivery.php?ID=047093101091070107064125087097081067010037073076067052094083124127029028113084004126099054038127042010098068091124111003064095098048031000085087000099004069103085109004086041084023080094065065004082025126099001093014027103064118088011085096000103004078&EXT=pdf

https://www.publico.pt/2018/07/03/sociedade/noticia/acesso-irregular-a-dados-clinicos-no-hospital-do-barreiro-vai-ser-investigado-1836751

https://sol.sapo.pt/artigo/549734/piratas-informaticos-atacam-hospital-garcia-de-orta-

https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact

LEGISLAÇÃO E JURISPRUDÊNCIA CONSULTADA

Código Civil

Convenção Europeia dos Direitos do Homem

Constituição da República Portuguesa

Decreto-Lei n.º 71/2007, de 27 de Março. Diário da República n.º 61/2007, Série I de 2007-03-27

Decreto-Lei n.º 18/2017 de 10 de fevereiro. Diário da República n.º 30/2017, Série I de 2017-02-10

Decreto-Lei n.º 133/2013, de 03 de outubro. Diário da República n.º 191/2013, Série I de 2013-10-03

Decreto-Lei n.º 157/99, de 10 de Maio. Diário da República n.º 108/1999, Série I-A de 1999-05-10

Decreto-Lei n.º 124/2011, de 29 de dezembro. Diário da República n.º 249/2011, Série I de 2011-12-29

Decreto-Lei n.º 446/85, de 25 de Outubro. Diário da República n.º 246/1985, Série I de 1985-10-25

Diretiva (EU) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016

Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, 24/10/95

Lei n.º 67/98, de 26 de outubro. Diário da República n.º 247/1998, Série I-A de 1998-10-26

Lei n.º 26/2016, de 22 de Agosto. Diário da República n.º 160/2016, Série I de 2016-08-22

Lei n.º 12/2015 de 26 de janeiro. Diário da República n.º 17/2015, Série I de 2015-01-26

Lei n.º 48/90, de 24 agosto. Diário da República n.º 195/1990, Série I de 1990-08-24

Lei n.º 43/2004 de 18 de Agosto. Diário da República n.º 194/2004, Série I-A de 2004-08-18

Lei n.º 148/2015, de 9 de setembro. Diário da República n.º 176/2015, Série I de 2015-09-09

Lei n.º 67/2007, de 31 de dezembro. Diário da República n.º 251/2007, Série I de 2007-12-31

Portaria n.º 147/2016 de 19 de maio. Diário da República n.º 97/2016, Série I de 2016-05-19

Portaria n.º 247/2000 de 8 de Maio. Diário da República n.º 106/2000, Série I-B de 2000-05-08

Proposta de Lei n.º 120/XIII

Regulamento Geral de Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

Acórdão do TC, de 01.04.1992, Nº 128/92, relator: Messias Bento

Acórdão do STJ, de 16/10/2014, proferido no Processo n.º 679/05.7TAEVR.E2.S, relator: Helena Moniz

Sentença do Processo n.º 2188/09.6TJLSB do 5º Juízo, 3ª secção dos Juízos Cíveis de Lisboa, proferida a 31 de Dezembro de 2010;

Sentença do Processo n.º 2393/09.5YXLSB do 7º Juízo, 3ª Secção dos Juízos Cíveis de Lisboa, proferida a 27 de Janeiro de 2011;

Sentença do Processo n.º 1810/09.9TJLSB, Juízos Cíveis de Lisboa, proferida a 10 de julho de 2012;