Irina Sofia Rodrigues Fernandes Bastos

PROTEÇÃO DE DADOS E DOCUMENTOS ADMINISTRATIVOS

ANÁLISE DO RGPD E ESTUDO DE CASO NA DIVISÃO ADMINISTRATIVA E DE RECURSOS HUMANOS DA CÂMARA MUNICIPAL DE VIANA DO CASTELO

Dissertação de Mestrado em Ciência da Informação, orientada pela Professora Doutora Liliana Isabel Esteves Gomes, apresentada ao Departamento Filosofia, Comunicação e Informação da Faculdade de Letras da Universidade de Coimbra

.

Junho de 2022

FACULDADE DE LETRAS

PROTEÇÃO DE DADOS E DOCUMENTOS ADMINISTRATIVOS

ANÁLISE DO RGPD E ESTUDO DE CASO NA DIVISÃO ADMINISTRATIVA E DE RECURSOS HUMANOS DA CÂMARA MUNICIPAL DE VIANA DO CASTELO

Ficha Técnica

Tipo de trabalho	**Dissertação**
Título	**Proteção de Dados e Documentos Administrativos**
Subtítulo	**Análise do RGPD e estudo de caso na Divisão Administrativa e de Recursos Humanos da Câmara Municipal de Viana do Castelo**
Autora	**Irina Sofia Rodrigues Fernandes Bastos**
Orientadora	**Liliana Isabel Esteves Gomes**
Júri	**Presidente: Doutora Maria Cristina Vieira de Freitas** **Vogais:** **Doutora Marta Diana Nunes Brandão** **Doutora Liliana Isabel Esteves Gomes**
Identificação do Curso	**2º Ciclo em Ciência da Informação**
Área científica	**Ciência da Informação**
Data da defesa	**15/07/2022**
Classificação	**18 valores**

1 2 9 0 FACULDADE DE LETRAS UNIVERSIDADE D COIMBRA

DEDICATÓRIA

Dedico este trabalho à grande mulher da minha vida … minha querida avó!

No coração guardo memórias que construí ao teu lado: *Ad infinitum*.

Amada Avó, obrigada por me ensinares lições tão valiosas e importantes. Contigo aprendi que a vida não é feita apenas de momentos bons e alegres, mas também de dificuldades. Estiveste sempre comigo e sempre estarás no meu coração.

As tuas palavras, os teus abraços, a tua voz doce, o teu sorriso… tudo isso faz parte de mim e será lembrado todos os dias.

Avó, Obrigada, Amo-te eternamente!

AGRADECIMENTOS

Esta dissertação de mestrado decorre de uma experiência única e reúne contributos de várias pessoas. Como tal, agradeço a disponibilidade, acompanhamento cuidado e colaboração demonstradas por todas as pessoas que fizeram com que este trabalho se tornasse possível.

Agradeço à minha família, pela paciência e apoio, que sempre me incentivou a aceitar o desafio de me inscrever no Mestrado em Ciência da Informação, contribuindo para o meu desenvolvimento pessoal e profissional.

Um especial agradecimento à minha querida orientadora, Professora Doutora Liliana Isabel Esteves Gomes, que sempre acreditou em mim. Pela sua orientação exemplar, pautada por um elevado rigor científico, um interesse permanente, uma visão crítica e oportuna, um empenho precioso e incansável, os quais contribuíram para enriquecer, com muita dedicação, passo a passo, todas as etapas do meu trabalho.

À chefe de divisão de Recursos Humanos e também amiga, Dr.ª Hirondina Machado, agradeço o apoio e motivação incondicional, que ajudou a tornar este trabalho uma válida e agradável experiência de aprendizagem.

Às minhas amigas e colegas de trabalho, Marlene e Ana, pela força, coragem e conselhos preciosos, total disponibilidade e encorajamento naqueles momentos mais difíceis.

Ao meu marido e filho, pelo amor, partilha, companheirismo e apoio incondicional. Agradeço-vos a enorme compreensão e generosidade, contribuindo para chegar ao fim deste percurso.

Por fim, o meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta dissertação, estimulando-me intelectual e emocionalmente.

RESUMO

A adaptabilidade, em conformidade, ao Regulamento Geral sobre a Proteção de Dados (RGPD) pelas organizações tem-se revelado um processo moroso e de grande complexidade, uma vez que existe a necessidade de equacionar distintas realidades organizacionais, não colocando em causa direitos e obrigações legais dos cidadãos.

Neste contexto, destacam-se os princípios da administração aberta e da proteção de dados, face os critérios de proporcionalidade (finalidade). Ou seja, existe a premência de uma análise contínua, originando o veto ou permissão de acesso aos documentos administrativos nominativos.

O presente estudo tem como objetivo geral analisar e compreender o RGPD na sua aplicabilidade organizacional na Administração Pública (AP). Especificamente, pretende-se: identificar as regras respeitantes ao tratamento de dados pessoais na União Europeia; estudar os conceitos, as categorias, os direitos e os princípios subjacentes; analisar o direito à proteção de dados pessoais na AP e concretizar um estudo de caso na Divisão Administrativa e de Recursos Humanos (DARH) da Câmara Municipal de Viana do Castelo (CMVC).

A metodologia qualitativa adotada compreende a pesquisa exploratória. O estudo de caso concretizou-se com recurso à pesquisa descritiva, análise de documentos internos e entrevista.

Dos resultados obtidos destacam-se propostas de melhoria, embora com a ressalva de que se trata de um trabalho em constante desenvolvimento. Nomeadamente: sensibilizar e formar os colaboradores para questões de privacidade, responsabilidade profissional e segurança informática em geral; necessidade de implementar um procedimento uniformizado e integral de tratamento e gestão de documentos administrativos; monitorizar o tratamento de dados pessoais sensíveis, no âmbito dos diferentes processos na DARH da CMVC.

Conclui-se que a operacionalidade da AP é norteada pelos princípios fundamentais estipulados no RGPD e na Lei de Proteção de Dados, destacando-se um trabalho exaustivo e em contínuo, por forma a garantir a conformidade e licitude do tratamento de todos os dados pessoais.

Palavras-chave: Proteção de dados; Documentos administrativos; Regulamento Geral sobre a Proteção de Dados (RGPD); Dados pessoais; Recursos Humanos.

ABSTRACT

The adaptability, accordingly, to the General Data Protection Regulation (GDPR) by organisations has proven to be a lengthy and complex process, since there is a need to consider different organisational realities, without putting into question the legal rights and obligations of citizens.

In this context, the principles of open administration and data protection stand out, given the criteria of proportionality (purpose). In other words, there is the urgency of a continuous analysis, originating in the veto or permission of access to nominative administrative documents.

The present study has the overall objective of analysing and understanding the GDPR in its organisational applicability in Public Administration (PA). Specifically, it aims to: identify the rules regarding the processing of personal data in the European Union; study the underlying concepts, categories, rights and principles; analyse the right to the protection of personal data in PA and carry out a case study in the Administrative and Human Resources Division (DARH) of the Municipality of Viana do Castelo (CMVC).

The qualitative methodology adopted comprises exploratory research. The case study was carried out using descriptive research, analysis of internal documents and interview.

The results obtained highlight proposals for improvement, although with the caveat that this is a work in constant development. Namely: to raise awareness and to train employees in matters of privacy, professional responsibility and computer security in general; the need to implement a uniform and integral procedure for the treatment and management of administrative documents; to monitor the treatment of sensitive personal data in the scope of the different processes in the DARH of the CMVC.

It is concluded that the operation of the PA is guided by the fundamental principles stipulated in the GDPR and in the Data Protection Law, highlighting an exhaustive and continuous work in order to ensure the compliance and lawfulness of the processing of all personal data.

Keywords: Data protection; Administrative documents; General Data Protection Regulation (GDPR); Personal data; Human Resources.

LISTA DE SIGLAS, ACRÓNIMOS E ABREVIATURAS

AEPD	Autoridade Europeia para a Proteção de Dados
AIPD	Avaliação de Impacto sobre a Proteção de Dados
AP	Administração Pública
APD	Autoridade Proteção de Dados
APDSI	Associação para a Promoção e Desenvolvimento da Sociedade da Informação
art.º	artigo
CADA	Comissão de Acesso a Documentos Administrativos
CCP	Código dos Contratos Públicos
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CE	Conselho Europeu
CI	Ciência da Informação
CEDH	Convenção Europeia dos Direitos do Homem
CEE	Comunidade Económica Europeia
CEPD	Comité Europeu para a Proteção de Dados
CIM Alto Minho	Comunidade Intermunicipal do Alto Minho
CMVC	Câmara Municipal de Viana do Castelo
CNPD	Comissão Nacional de Proteção de Dados
CNPDPI	Comissão Nacional de Proteção de Dados Pessoais Informatizados
CPA	Código do Procedimento Administrativo
CRP	Constituição da República Portuguesa
CT	Código de Trabalho
D95	Diretiva 95/46/CE
DARH	Divisão Administrativa e de Recursos Humanos
DGLAB	Direção-Geral do Livro, dos Arquivos e das Bibliotecas
DPO	*Data Protection Officer*
DUDH	Declaração Universal dos Direitos do Homem
EM	Estados Membros
ERP	*Enterprise Resource Planning*
EPD	Encarregado de Proteção de Dados
EU	*European Union*
GD	Gestão Documental
GDPR	*General Data Protection Regulation*
GRH	Gestão de Recursos Humanos
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
IAPD	Informação Administrativa e Proteção de Dados

IEC	*International Electrotechnical Commission*
IP	*Internet Protocole*
ISO	*International Organization for Standardization*
LC	Lista Consolidada para a classificação e avaliação da informação pública
LPDP	Lei de Proteção dos Dados Pessoais
n.º	número
PAA	Princípio da Administração Aberta
PRACE	Programa de Reestruturação da Administração Central do Estado
PRCON	Procedimento concursal
PREMAC	Plano de Redução e Melhoria da Administração Central
PT	Portugal
RAMP	*Records and Archives Management Programme*
RGPD	Regulamento Geral de Proteção de Dados
RH	Recursos Humanos
SAP	Secção Administrativa de Pessoal
SGD	Sistemas de Gestão Documental
SGQ	Sistema de Gestão da Qualidade
SGSI	Sistema de Gestão e de Segurança da Informação
SI	Sociedade da Informação
TIC	Tecnologias da Informação e de Comunicação
TPF	Tipo de Processo de Funcionário
TSFUE	Tratado sobre o Funcionamento da União Europeia
UE	União Europeia

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

SUMÁRIO

INTRODUÇÃO

O presente trabalho foi elaborado no âmbito do Mestrado em Ciência da Informação (CI), da Faculdade de Letras da Universidade de Coimbra.

Encarou-se este estudo como um desafio estimulante a nível profissional, visto tratar-se de um tema atual e de certa forma problemático, uma vez que o Regulamento Geral sobre a Proteção de Dados (RGPD) entrou em vigor em 24 de maio 2016 e é aplicável desde 25 de maio 2018 em todas as organizações europeias, que tratem dados pessoais de cidadãos europeus ou em espaço europeu.

O RGPD, tanto na conjuntura europeia como em cada um dos Estados-Membros (EM), vem robustecer a ideia que já existia de proteção de dados, num cenário evolutivo em termos de contexto jurídico-legal e vem exigir a reformulação de alguns aspetos, face ao progresso tecnológico, por forma a prevalecer a primazia do titular de dados pessoais sobre o seu direito fundamental à privacidade.

A obrigação de aplicar o RGPD nas organizações exigiu a adoção de ferramentas para proteger todos os titulares de dados pessoais e não a entidade por si só, algo que já se presumia pelo art.º 8 da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

Sinteticamente, este regulamento tem como foco principal, segundo o Conselho da União Europeia (UE) e do Conselho Europeu (CE) (2020): instituir-se normativamente em todos os EM, acompanhando o desenvolvimento tecnológico evolutivo, em resposta à ameaça e utilização imprópria dos dados pessoais por parte das organizações; aumentar a proteção e apoiar o projeto de mercado único digital, livre e seguro, promovendo a eliminação das barreiras fronteiriças na UE.

Neste contexto, como objetivo geral desta dissertação pretende-se: analisar o RGPD e compreender a sua aplicabilidade na Administração Pública (AP). Os objetivos específicos são: identificar as regras relativas ao tratamento de dados pessoais na UE; estudar conceitos, categorias, direitos e princípios subjacentes; analisar o direito à proteção de dados pessoais na AP; concretizar um estudo de caso na Divisão Administrativa e de Recursos Humanos (DARH) da Câmara Municipal de Viana do Castelo (CMVC).

A metodologia qualitativa adotada nesta investigação compreende: revisão de literatura, mediante pesquisa acerca das temáticas RGPD, Dados Pessoais, Proteção de Dados na AP, Documentos Administrativos e Gestão Documental; o estudo de caso concretizou-se com recurso à pesquisa descritiva, análise de documentos internos e entrevista.

Foi fundamental realizar uma revisão de literatura, com o intuito da demarcação da problemática em estudo e determinação do percurso investigativo. O objeto de investigação que emergiu insere-se num contexto organizacional específico.

Este trabalho compreende, no primeiro capítulo, a análise da evolução legislativa e normativa europeia e nacional, bem como o âmbito e objetivos do RGPD e as funções da Comissão Nacional de Proteção de dados (CNPD). No capítulo seguinte investigamos o progresso das formas de tratamento dos dados pessoais em contexto de trabalho, as suas categorias, princípios, direitos e consentimentos.

Examinando o RGPD através da Lei n.º 59/2019, de 8 de agosto apresentamos os princípios indispensáveis para o tratamento de dados pessoais: Princípio da licitude e da lealdade; Princípio da limitação das finalidades; Princípio da minimização dos dados; Princípio da exatidão; Princípio da limitação da conservação; Princípio da integridade e confidencialidade; Princípio da responsabilidade e o Princípio do consentimento.

O consentimento do titular dos dados é apenas um, entre muitos trâmites de legitimidade previstos no processo de tratamento destes dados pelo RGPD. Ou seja, em cada finalidade de tratamento de dados equacionado é importante corresponder a necessidade de consentimento ou não, salvaguardando a licitude. Importa assim, confrontar se há outro fundamento de legitimidade previsto pelo suporte legal (RGPD) para legitimar este tratamento.

No Código do Trabalho (CT) encontra-se salvaguardada a proteção dos dados pessoais e da vida privada, contudo o RGPD conduziu a uma proteção mais minuciosa e específica ao trabalhador, nas várias normas a ter em conta no momento do tratamento dos seus dados pessoais. Numa primeira instância, o empregado está mais protegido e o empregador necessita definir vários autodomínios, por forma a garantir que atinge todos os parâmetros, estabelecendo uma segurança mútua de acordo com a legalidade.

O RGPD na AP, a Gestão Documental (GD) e o acesso a documentos administrativos em face da proteção de dados são as temáticas abordadas no terceiro capítulo.

A AP também se encontra sujeita às regras do RGPD, "no âmbito das suas competências e atribuições conferidas por lei aos serviços públicos", tendo a "legitimidade para tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD", particularmente "tratamento equitativo e lícito, limitação da finalidade, minimização dos dados e conservação dos dados" (Teves, 2019, p. 101).

As atuais tecnologias digitais permitem a adoção de *softwares* na GD, que sustentam a gestão dos sistemas tecnológicos e a tramitação de uma diversidade de documentos eletrónicos (Nguyen, Swatman & Fraunholz, 2007).

Neste contexto, torna-se impreterível que na GD as organizações desenvolvam e implementem políticas, estratégias e ferramentas que apoiem transversalmente processos como: meios de

autenticação eletrónica; gestão de procedimentos e de instrumentos de *workflow*; gestão de emails, de conteúdos, de arquivo e de risco, entre outros (Pinto, 2013).

O objetivo da GD passa pelo domínio da produção, conservação e avaliação de "records", ou seja, documentos gerados e recebidos dentro de uma organização (pública ou privada) no decorrer da sua operacionalidade, sendo desta forma preservados, como prova (Webster *et al*., 1999, cit. por Pinto, 2013).

Como benefícios práticos da implementação da GD descortina-se a otimização do trabalho de arquivo, a preservação, a conservação e a recuperação rápida de documentos/informação, a possibilidade da adição célere de documentos/informação, a otimização e libertação dos espaços físicos, o controlo dos procedimentos documentais e a simples partilha ou eliminação dos documentos (Calderon, Cornelsen, Pavezi & Lopes, 2004).

A Gestão de Informação é "uma área transversal e interdisciplinar que tem para a CI uma dimensão aplicacional" (Gomes, 2016, p. 144) e incorpora a GD, tornando-se essencial nas organizações, existindo uma interligação entre o seu ciclo de vida e a gestão de conteúdos (Pinto & Silva, 2005). Neste contexto, a norma ISO 26122 ao reger a GD, centra o seu objetivo de acompanhar o ciclo de vida integral de um documento, que pode adotar diferentes formas e ser analisado de forma individual, desde a produção à preservação ou eliminação (Pinto, 2013).

Subsiste, desta forma, a premência de um Sistema de Gestão de Documentos (SGD), que segundo Shipman (1999) é um sistema que domina: a conceção, o armazenamento, a partilha, a disponibilização e o procedimento de atualização destes documentos, bem como, o controlo do *check-in*, *check-out* e a revisão dos documentos. Por fim, aporta também a simplificação do manuseamento documental (Silva, 2000), sublinhando a vertente informática de gestão.

O SGD inclui, administra e provê acesso aos documentos integrados, numa abordagem geral e sistemática dentro das organizações, onde se encontram interligados documentos, condutas e políticas. Com a implementação prática do SGD, o plano estratégico atinge o seu fim e, consequentemente, é possível uma apreciação contínua que possibilita controlar erros e adotar melhorias. Mas, para que este processo seja útil é fundamental clarificar as responsabilidades, com o apoio da gestão de topo, através da definição de uma política de GD. É, deste modo, possível uma gestão integrada do arquivo, onde estão compreendidas todas as exigências práticas, tomando como referência o contexto normativo (António, 2009).

Em termos práticos, no último capítulo analisamos a proteção de dados, especificamente na DARH da CMVC. Após uma breve contextualização, refletimos sobre o sistema de GD na área dos

recursos humanos, o que nos leva a debruçar nas funcionalidades do *software* utilizado pela CMVC, o e-*SigGOV*, que gere todos os trâmites e informação/documentos.

A plataforma *e-SigGov* materializa-se num *software* de gestão de documentos que permite a organização dos mesmos num sistema cronológico, com tempos e configurações de execução e acessos, em tempo real, tornando palpável a desmaterialização de processos.

Assim, no estudo de caso procurámos analisar a importância da recolha e do tratamento de dados pessoais, verificando se os mesmos estão em conformidade com o RGPD; caracterizar o *e-SigGOV* e verificar se o mesmo preenche os requisitos técnicos para suporte da GD e integração do RGPD. Por fim, concluímos com uma reflexão crítica, propostas de melhoria e destacamos o contributo do profissional de informação.

Em suma, salienta-se que existe sempre a necessidade de encontrar um equilíbrio entre o que torna a AP mais ágil no desenvolvimento dos seus procedimentos e prestação de serviços ao cidadão, sem colocar em causa a licitude e conformidade da adaptabilidade ao RGPD.

1. O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS

1.1 EVOLUÇÃO LEGISLATIVA E NORMATIVA

Este capítulo aborda a evolução legislativa e normativa da Privacidade à Proteção de Dados, o âmbito e os objetivos do RGPD e as funções da CNPD.

Com o aumento da utilização das ferramentas tecnológicas incrementou-se a disseminação de dados privados dos indivíduos, algo impensável para a humanidade noutros tempos. Mendes (2014) relembra que este tema despoletou num artigo sobre a privacidade, pelos autores Warren e Brandeis, intitulado *"The right to privacy".*

A questão sobre a informação e dados conservados em bases de dados e a sua salvaguarda surge em meados do século XX, quando a relevância da privacidade começou a ter maior destaque no cenário do direito europeu e internacional. Destacam-se, seguidamente (quadro 1), os diplomas, regulamentos e entidades mais relevantes, na evolução legislativa europeia.

Quadro 1: Evolução do sistema normativo europeu, com relevância na privacidade

Data	Entidade / Diploma	Notas contextuais
1950	Conselho da Europa	Abraçou a Convenção Europeia dos Direitos do Homem (CEDH), onde foi declarado: "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência" (art.º 8º).
1957	Tratado de Roma	Este tratado conduziu à origem da Comunidade Económica Europeia (CEE) que instituiu um mercado europeu comum e por conseguinte, a legislação análoga em substância de tratamento de dados.
A ideia pré-concebida neste período era que, como só os centros computacionais de grande envergadura lidavam com controlo de dados, logo se existia alguma violação, esta partiria destes casos (Vieira, 2007). Pelo que, neste contexto, os governos centravam os seus esforços através da atribuição de autorização a essas entidades, para suportarem a privacidade. O que resultou numa situação de total falta de controlo, tanto por parte destas entidades, como dos governos.		
1981	Convenção nº 108, Conselho da Europa	Instituiu várias medidas no que respeita ao procedimento automatizado de dados de caráter pessoal. Esta convenção vem dar resposta face aos enormes avanços tecnológicos informativos e a necessidade crescente de adequar a proteção dos direitos individuais (Saldanha, 2019).

Neste contexto e após todas as diligências projetadas, a multiplicidade jurídica dos diferentes Estados-Membros (EM), dava azo a incertezas no que respeita às adaptações necessárias face à importância de harmonização normativa.		
1995	Diretiva 95/46/CE, Parlamento Europeu (PE) e Conselho Europeu (CE)	Para dar resposta a esta necessidade de consonar todas a diferentes legislações vigentes nos EM, apresentou-se esta diretiva que se foca na proteção das pessoas singulares, no tratamento dos seus dados pessoais e à sua livre circulação. Que vigorou até ao dia 25 de maio de 2018. A deliberação desta diretiva marca uma renovação de mentalidades, bem como, uma sensibilização maior para a proteção de dados. Ao ser uma diretiva europeia torna-se vinculativa e consequentemente há a necessidade de que cada estado-membro, a acomode à sua legislação nacional.
	art.º 29º e 30º, Diretiva 95/46/CE	O Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (GT29) foi instituído pelo art.º 29 da presente diretiva, que emite recomendações e pareceres. Trata-se de um órgão independente de proteção de dados e privacidade. Este é integrado por representantes das autoridades nacionais dos EM da UE. Futuramente é substituído pelo Comité Europeu para a Proteção de Dados (CEPD), nos termos do RGPD.
2000	CDFUE	Convenciona: "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (art.º 8, Carta dos Direitos Fundamentais da União Europeia (CDFUE)).
2001	Regulamento (CE) n.º 45/2001	Relativo ao tratamento de dados pessoais por instituições e órgãos comunitários.
2002	Diretiva 2002/58/CE	Quanto à privacidade (alterada em 2009).
2004	Criação da Autoridade Europeia para a Proteção de Dados (AEPD)	A UE sentiu necessidade da criação de uma entidade europeia de controlo, que garantisse que a globalidade das instituições e organismos da UE, honrassem o direito à privacidade dos cidadãos, durante o processamento dos seus dados pessoais (AEPD, 2021).
2006	Diretiva 2006/24/CE	Relativa à conservação de dados.
2007	Tratado de Lisboa	O Tratado de Lisboa foi assinado em 2007 (harmonizou as competências legislativas entre o CE e o PE) e entra em vigor em 2009, garantindo a proteção de dados um direito fundamental. A partir deste marco há base jurídica específica e consonância com o instituído pela Carta dos Direitos Fundamentais da UE.

2008	Decisão-Quadro 2008/977/JAI do Conselho	Relativo à proteção de dados pessoais tratados no âmbito da cooperação policial e judiciária de matéria penal. Futuramente revogada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
2011	AEPD	Emissão de um parecer instituindo a carência de legislação em proteção de dados e sugestões de propostas de melhoramento. Estimula a proatividade da CE na criação de novos regulamentos, a procura de colaboração e o autodomínio de conformidade.
2015	CE, com recomendações da AEPD	Entra-se numa abordagem geral sobre o Regulamento Geral de Proteção de Dados (RGPD) ou *General Data Protection Regulation (GDPR),* pelo CE e recomendações da AEPD sobre o texto final.
2016	Diploma 2016/679, PE e o CE	O CE, PE e Comissão chegam a acordo. É delineado o planeamento para a efetivação do RGPD, aprovado pelo PE e o Conselho do RGPD (Regulamento UE 2016/679), entrando em vigência 20 dias depois da publicação no Jornal Oficial da UE.
	Regulamento (UE) 2016/679	Criação do CEPD; deste regulamento: Consideração 72; Artigo 68, secção 3 do Capítulo VII e Artigo 94. Capítulo XI. Aplicável no dia 25 de maio 2018, em todos os países membros da UE. Este é um organismo da UE encarregado da aplicação do RGPD. É composto pelo chefe de cada Autoridade Proteção de Dados (APD) e da AEPD ou pelos seus representantes.
	Regulamento (UE) 2016/680	Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Aplicável no dia 6 de maio 2018, em todos os países membros da UE.
2018	Regulamento (UE) 2018/1725	Este regulamento define as regras aplicáveis no tratamento de dados pessoais pelas instituições, organismos e agências da União Europeia, em consonância com o disposto no RGPD e Diretiva sobre a Proteção de Dados na Aplicação da Lei. Este regulamento entrou em vigor em 11 de dezembro de 2018.
		Várias considerações neste regulamento. A AEPD é um organismo independente da UE, responsável por presenciar a aplicação das regras, em matéria de proteção de dados, nas instituições europeias e dar acompanhamento às reivindicações.
		Criou o Responsável pela Proteção de Dados (RPD) que garante, de forma independente, o correto emprego da legislação, em matéria de proteção de dados pessoais, pelo CE e

		mantém um registo público, de todas as operações realizadas pela Comissão, que incluam o tratamento de dados pessoais. Coopera com a AEPD.

Fonte: Elaboração própria.

A atual conjuntura de globalização e grandes avanços tecnológicos veio impor uma atualização no processo de tratamento dos dados pessoais (de pessoas singulares) e a sua livre circulação. Esta realidade evolutiva permite a partilha e o armazenamento informático automatizado de forma fácil e rápida. Este cenário de progresso digital em termos económicos e tecnológicos acarreta não apenas benefícios, mas também consequências na perda de controlo na transmissão destes dados (Cunha, Hierro & Silva, 2020). A resposta a esta questão chega-nos através do RGPD que permite controlar a evolução deste mercado único digital, que assenta na base de extinção de barreiras à livre circulação de mercadorias, pessoas, serviços e capitais, entre os EM da UE.

Este tema foi abordado pela primeira vez em Portugal, na Constituição de 1976, que instituía o direito dos cidadãos a um registo mecanográfico pessoal, atribuindo poderes de exigir a sua retificação e atualização. Bem como, a "informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos" (art.º 35, nº2, Constituição da República Portuguesa (CRP)).

Sumariamente destacam-se seguidamente os diplomas e leis de adaptação mais relevantes, na evolução legislativa portuguesa.

Quadro 2: Evolução legislativa em Portugal, com relevância na privacidade

UE	PT	Notas contextuais
	Lei n.º 10/91	Só 15 anos mais tarde, é que Portugal patenteia a primeira Lei de proteção dos dados pessoais. Esta ainda é muito distinta pela questão informática e o procedimento automatizado dos dados pessoais. Aqui são instauradas as penalizações judiciárias primordiais, bem como a criação da **Comissão Nacional de Proteção de Dados Pessoais Informatizados** (CNPDPI), a responsável nacional para a matéria da proteção de dados.
	Lei n.º 28/94	Após 3 anos surge uma nova Lei, que fortifica a carência de proteção dos dados pessoais, e confere à CNPDI o direito à informação e acesso aos dados pessoais.

Diretiva 95/46/CE	**Lei n.º 67/98**	Esta lei viabilizou a adaptação imperativa da diretiva europeia em Portugal e introduz as conceções presentes no RGPD: • Tratamento lícito dos dados; • O tratamento deve ser feito para as finalidades específicas; • Os dados recolhidos devem ser adequados e pertinentes; • Os dados devem ser exatos; • Surge o Direito ao Apagamento e o Direito de não ficar sujeito a decisões automatizadas;
2004	**Lei n.º 41/2004**	Aqui aborda-se mais especificamente a área de redes e serviços de comunicações eletrónicas acessíveis ao público. Alterada pela Lei n.º 46/2012, de 29 de agosto.
	Lei nº 43/2004	Esta conjetura lata na regulação da proteção de dados pessoais, impõe a necessidade de adequar a Autoridade Nacional às novas tendências. Regula no âmbito organizacional e funcionamento da Comissão Nacional de Proteção de Dados (CNPD), bem como, o estatuto pessoal dos seus membros. Atualizada pelo art.º 43, Lei n.º 59/2019.
2012	**Lei n.º 46/2012**	Institui na vertente da área de redes e serviços de comunicações eletrónicas acessíveis ao público.
Regulamento (UE) 2016/680	**Lei n.º 59/2019**	Sanciona as regras de tratamento de dados pessoais, com efeitos preventivos, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais.
		O art.º 43 designa a CNPD como a tutela responsável do RGPD e da lei que agora entra em vigor.
Diretiva (UE) 2016/679, PE e CE	**A Lei n.º 58/2019**	Esta é a nova Lei de Proteção de Dados, que assegura a execução do RGPD na ordem jurídica portuguesa. Entrou em vigor no dia 9 de agosto e revoga a anterior (Lei n.º 67/98). Procede ainda às alterações à Lei n.º 43/2004 (republicada), no que respeita à organização e o funcionamento da CNPD, bem como, à Lei n.º 26/2016, que homologa o regime de acesso à informação administrativa e ambiental e do seu reaproveitamento.
		Há três razões para a existência desta nova Lei face ao RGPD, designadamente: 1. transmite aos EM a determinação sobre algumas matérias específicas, como por exemplo: tratamento de dados dos trabalhadores, idade mínima de menores, etc. 2. demarca que cada Estado-Membro nomeie por ato legislativo, a autoridade de fiscalização incumbida do seu emprego.

		3. as normas sobre as contraordenações não são diretamente aplicáveis, impondo-se a necessidade de adequação por ato legislativo nacional, (Universidade de Coimbra (UC), 2021).
		EPD art.º 9º a 13º do Capítulo III.
		Enquanto o art.º 14 do Capítulo IV, prevê a cooperação com o Instituto Português de Acreditação, I. P., em matéria de acreditação dos organismos de certificação.
	Proposta de Lei n.º 120/XIII	Visa atestar a execução na ordem jurídica nacional, relativo ao tratamento de dados pessoais e à sua livre circulação. O RGPD irá por sua vez anular a Lei n.º 67/98 e permutar as competências da CNPD, neste domínio. Deu origem ao Texto de Substituição da Proposta de Lei n.º 120/XIII/3.ª.

Fonte: Elaboração própria.

Decorrente da análise da informação sistematizada no quadro 2, considera-se que a implementação do RGPD, tanto na conjuntura europeia como nos EM, vem robustecer a proteção de dados pessoais, mediante um percurso evolutivo em termos de peso no contexto jurídico-legal e reformulação em alguns aspetos, face ao progresso tecnológico, por forma a prevalecer a primazia do titular de dados pessoais sobre o seu direito fundamental à privacidade.

A *International Organization for Standardization* (ISO) ou Organização Internacional de Normalização é uma organização independente e não governamental, com 165 organismos nacionais de normalização, com a finalidade de promover a qualidade de produtos e serviços. Esta é uma das maiores instituições que desenvolve normas a nível mundial, e foi criada a partir da união da *International Federation of the National Standardizing Associations* e *United Nations Standards Coordinating Committee*. Começou a laborar de forma oficial em 1947 (ISO, 2021).

Quanto às normas ISO sobre as matérias de proteção de dados pessoais e dos sistemas de gestão da segurança da informação, destacam-se as seguintes (quadro 3).

Quadro 3: Normas ISO/IEC

ISO/IEC	
A ISO/IEC 29100:2011	O quadro de privacidade (parafraseado da versão em inglês, ISO/IEC 29100:2011) destina-se a ajudar as organizações a definir os seus requisitos de salvaguarda da privacidade relacionados, com a informação pessoalmente identificável dentro de um ambiente TIC:

	• Especifica a terminologia comum de proteção da privacidade; • Define os atores e os papéis no processamento de informações que identificam pessoalmente; • Descreve os requisitos de salvaguarda da privacidade; • Referencia os princípios de privacidade conhecidos.
ISO/IEC 27005:2011	Estabelece as diretrizes de suporte e orientação na gestão de riscos de segurança da informação. Esta norma é aplicável (parafraseado da versão em inglês, ISO/IEC 27005:2011) a todas as organizações (como é o caso, empresas comerciais, agências governamentais, organizações sem fins lucrativos) que tencionam gerir riscos que comprometam a segurança da informação da organização.
ISO/IEC 27001:2013	Estabelece as condições (parafraseado da versão em inglês, ISO/IEC 27001:2013) para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação, dentro do contexto da organização. A adoção deste sistema é uma decisão estratégica para uma organização e o seu estabelecimento e implementação é influenciado pelas suas necessidades e objetivos (segurança, processos utilizados), bem como, a sua dimensão e estrutura.
ISO/IEC 29134:2017	Disponibiliza um guia para preceder a avaliações e respetivo relatório de impacto de privacidade. Uma avaliação do impacto na privacidade (parafraseado da versão em inglês, ISO/IEC 29134:2017) é um instrumento de avaliação de potenciais impactos na privacidade de um processo (através de um sistema de informação, programa, módulo de software, dispositivo ou outra iniciativa que processe informação pessoal identificável), para tomar as medidas necessárias a fim de tratar os riscos de privacidade.

Fonte: Elaboração própria.

Estas normas focam-se maioritariamente na atribuição de certificação às organizações, garantindo que estas normas são cumpridas. Ou seja, caso sejam auditadas quanto à proteção implementada ao tratamento de dados pessoais e às medidas de segurança na gestão dos riscos e avaliações de impacto, as organizações permanecem corretamente patenteadas/atestadas pelo RGPD e os modelos de qualidade essenciais. Tendo como objetivo a confiança do titular de dados pessoais, no tratamento destes, pela organização.

1.2 ÂMBITO E OBJETIVOS DO REGULAMENTO UE 2016/679

O RGPD foi formulado a 27 de abril de 2016, pelo Parlamento e Conselho Europeus. A sua plena aplicabilidade na UE verifica-se em 25 de maio de 2018 (3 anos depois), sendo que "todas as entidades, a ele sujeitas, são obrigadas a cumprir as normas previstas neste Regulamento" (Vieira, 2018, p. 1).

Com o objetivo de adequação para a legislação portuguesa, temos a Lei n.º 58/2019, de 8 de agosto, que assegura a execução na ordem jurídica nacional do Regulamento (UE) 2016/679, "relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (Lei n.º 58/2019, art.º 1.º). Em relação a esta Lei, importa referir:

1. As "normas relativas à proteção de dados pessoais previstas em legislação especial mantêm-se em vigor, em tudo o que não contrarie o disposto no RGPD e na presente lei" (art.º 62);

2. Altera o art.º 6.º do "regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos aprovado pela Lei n.º 26/2016";

3. Altera os artigos 2.º, 3.º, 8.º, 16.º a 19.º, 20.º (este último na redação da Lei n.º 55-A/2010, de 31 de dezembro), 21.º, 22.º e 24.º a 31.º, adita os artigos 19.º-A e 24.º-A e revoga o n.º 3 do art.º 15.º e o n.º 2 do art.º 17.º da Lei de Organização e Funcionamento da CNPD, aprovada pela Lei n.º 43/2004, de 18 de agosto;

4. Revoga a Lei n.º 67/98, de 26 de outubro.

Figura 1: Principais novidades da Lei n.º 58/2019

- Maior amplitude do conceito de dados pessoais;
- Direito ao esquecimento (apagamento), direito de portabilidade dos dados, direito ao consentimento e direito de oposição ao *profiling*;
- Reforço das obrigações das organizações;
- Regras especiais para menores;
- Obrigação de comunicar quebras de segurança;
- *Accountability*;
- EPD;
- Avaliação de Impacto sobre a Proteção de Dados (AIPD).

Fonte: Adaptado de "Informação Administrativa e Proteção de Dados" (UC, 2021).

Quanto à homologação das normas relativas ao "tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais", temos a Lei n.º 59/2019, que adota igualmente a Diretiva (UE) 2016/680.

O RGPD representa, segundo Magalhães (2018, p. 7), "uma mudança de paradigma no modelo de tratamento de dados pessoais e de livre circulação dos mesmos, com vista à garantia do mercado único sem restrições em virtude do diferente enquadramento legal e salvaguarda do direito à proteção dos dados pessoais".

Verifica-se na EUR-Lex (2020), na forma simples e detalhada, que o presente regulamento é desenvolvido com um único objetivo – melhorar o controlo dos dados pessoais. Contudo, também vem "modernizar e unificar regras que permitem às empresas reduzir burocracia e beneficiar de um maior grau de confiança por parte dos consumidores" (EUR-Lex, 2020, p. 1).

Vieira (2014, p. 1) acrescenta que o foco é igualar este regulamento nos respetivos EM, colocando o "acento tónico no titular dos dados", permitindo um desenvolvimento no Mercado Único Digital. É de citar que, num mundo de tal maneira tecnológico, o RGPD é igualmente aplicável a entidades que não se encontrem inseridas na UE, isto se estas expandirem atividades para a oferta de bens e serviços a cidadãos europeus, ficando indubitavelmente claro que o RGPD extravasa a UE (Magalhães, 2018).

Moreira (2018) relembra que, um dos objetivos primordiais é também a implementação de mecanismos legislativos associados à constante evolução tecnológica nos EM, aumentando assim a proteção dos titulares dos respetivos dados pessoais.

Pinheiro (2018) justifica que esta lei da proteção de dados é aplicada a quem procede ao tratamento de dados pessoais, quer sejam entidades privadas ou públicas, indivíduos jurídicos ou físicos, envolvendo componentes como:

- Processar-se no território nacional;
- Que o objetivo seja o fornecimento ou oferta de serviços e bens, ou então, que o tratamento destes dados seja localizado em território nacional;
- Os dados sejam coletados no território nacional.

O RGPD reitera nos seus artigos 2.º e 3.º (Lei n.º 58/2019, de 8 de agosto) o âmbito de aplicação no "território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento", e atribui autoridade à CNPD o "controlo nacional para efeitos do RGPD e da presente lei".

Esta Lei aplica-se ainda fora do território nacional, quando o tratamento de dados pessoais é efetuado: num "estabelecimento situado no território nacional" (art.º 2, nº 2, a), pertençam a "titulares de dados que se encontrem no território nacional" (art.º 2, nº 2, b) ou a "titulares portugueses residentes no estrangeiro" (art.º 2, nº 2, c).

Sendo assim, recaem sob o "chapéu" normativo do RGPD, todos os processos de tratamentos de dados de cidadãos (residentes ou não residentes na UE) e empresas (públicas ou privadas) que estejam instalados na UE ou fora dela.

São também alvo de aplicação do RGPD todos os responsáveis pelo tratamento de dados, seja o encarregado(s) de proteção de dados, o subcontratante(s) e todas as pessoas que participam em qualquer intervenção de tratamento de dados, "estão obrigados a um dever de confidencialidade que acresce aos deveres de sigilo profissional" (art.º 10, nº2).

É a combinação destas três formalidades que nos ajudam a absorver a imposição da implementação do RGPD numa entidade (Magalhães e Pereira, 2018). Então temos:

a) Organismo procede ao tratamento de dados pessoais;

b) Organismo em causa é responsável pelo tratamento e

c) Existe ligação geográfica do estabelecimento com a UE.

A obrigação de aplicar o RGPD nas organizações vem alterar substancialmente aspetos organizativos das mesmas. Resumidamente, este regulamento tem como foco principal, segundo o Conselho da UE e CE (2020):

- Instituir-se normativamente em todos os EM, acompanhando o desenvolvimento tecnológico evolutivo;
- Em resposta à ameaça e utilização imprópria dos dados pessoais por parte das organizações, aumentar a proteção;
- Apoiar o projeto de mercado único digital, livre e seguro, promovendo a eliminação das barreiras fronteiriças em toda a UE.

Este último ponto é muito importante, pelo que as últimas conclusões do Conselho da UE sobre a construção do futuro digital da Europa destacam a sua importância acrescida face à recuperação pós-COVID-19. Quanto aos domínios abrangidos pelas referidas conclusões salienta-se "a conectividade, as cadeias de valor digitais e a saúde em linha, até à economia dos dados, à inteligência artificial e às plataformas digitais" (Conselho da UE e Conselho Europeu, 2020).

1.3 COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

A CNPD (2021a) é uma entidade administrativa independente, com personalidade jurídica de direito público e com autoridade, provida de independência administrativa e financeira, que trabalha junto à Assembleia da República.

A CNPD é, portanto, a autoridade de controlo nacional para efeitos do RGPD, da Lei n.º 58/2019, de 8 de agosto, da Lei n.º 59/2019, de 8 de agosto e da Lei n.º 41/2004, de 18 de agosto, com as alterações introduzidas pela Lei n.º 46/2012, de 29 de agosto. Trata-se de uma entidade que controla e fiscaliza o cumprimento do RGPD e da Lei n.º 58/2019, de 8 de agosto "bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais" (CNPD, 2021a). As organizações têm a obrigação de colaborar com a CNPD, fornecendo a informação solicitada, como o acesso a sistemas informáticos, ficheiros e tratamento de dados pessoais.

A CNPD atua com "independência na prossecução das suas atribuições e competências (previstas, designadamente, nos artigos 57.º do RGPD, 6.º da Lei n.º 58/2019 e 44.º da Lei n.º 59/2019) e no exercício dos seus poderes (cf. Artigos 58.º do RGPD, 8.º da Lei n.º 58/2019 e 45.º da Lei n.º 59/2019)" (CNPD, 2021a).

Conforme já foi referido, numa primeira fase houve a necessidade de um período de adaptação muito grande para as organizações e diferentes instituições no país, pelo que a CNPD encorajou estas entidades (publicas e privadas) a que já se começassem a preparar a nível interno, para a implementação do RGPD. Tornando premente identificar as novas regras e obrigações, face ao utilizado até ao momento e proceder às adaptações necessárias.

Neste contexto, a CNPD identificou as dez áreas principais de atuação: 1. Informação aos titulares dos dados; 2. Exercício dos direitos dos titulares dos dados; 3. Consentimento dos titulares dos dados; 4. Dados sensíveis; 5. Documentação e registo de atividades de tratamento; 6. Contratos de subcontratação; 7. EPD; 8. Medidas técnicas e organizativas e segurança do tratamento; 9. Proteção de dados desde a conceção e avaliação de impacto e 10. Notificação de violações de segurança.

Salienta-se, ainda, que a partir deste momento torna-se também imperativo ter um EPD (ponto 7 anterior). A proteção de dados pessoais (físicos ou digitais), exige um reforço das medidas de proteção neste sentido, o que implica a supervisão dos fluxos de dados pessoais, o seu controlo e o aumento do nível de alerta face aos riscos de privacidade.

2. DADOS PESSOAIS E TRATAMENTO

2.1 CONCEITOS E CATEGORIAS

Neste capítulo explana-se a evolução do conceito de dados pessoais, categorias e respetivo tratamento, comparando a Diretiva 95/46/CE e o Regulamento (UE) 2016/679, já que este suplanta a sua aplicação. Identifica-se uma evolução do conceito dos dados pessoais, já que passa a abranger uma dimensão direta ou indireta, bem como, o elemento específico genético e mental. Quanto ao conceito de tratamento este manteve-se (quadro 4).

Quadro 4: Definição de dados pessoais e tratamento

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" (art.º 2, a), D 95).
	"informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada 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, indentificadores por via eletrónica ou a um ou mais elementos específicos da sua identidade física, fisiológica, **genética, mental**, económica, cultural ou social dessa pessoa singular" (art.º4, nº1, RGPD).
Tratamento	"qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha , registo, organização, conservação, adaptação ou alteração, recuperação, consulta , utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" (art.º 2, b), D 95).
	"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, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art.º 4, n.º 2, RGPD).

Fonte: D95 e RGPD.

Já segundo o Parecer nº 4/2007, do GT29 que foi instituído pela D95, existem quatro elementos que estão relacionados e apoiam-se mutuamente, quanto à definição de "dados pessoais". Neste contexto, vamos agora abordar cada uma das alíneas separadamente para melhor entendimento.

Quadro 5: Elementos relacionados quanto à definição de "dados pessoais"

Alíneas	Ideias delineadoras:
a) "Qualquer informação", (GT29, p. 6)	Os dados pessoais apresentam-se como um conceito alargado, que pode ser analisado segundo as perspetivas: 1) natureza da informação (estão incluídas qualquer tipo de testemunhos sobre uma determinada pessoa, ou seja, informações "objetivas" e "subjetivas" (GT29, p. 6)). 2) conteúdo da informação (inclui dados que provêm qualquer tipo de informação)
b) "Relativa a", (GT29, p. 9)	Trata-se de um componente crasso que garante o reconhecimento "com precisão, quais as relações/ligações relevantes e como distingui-las." (GT29, p. 9). A informação "relativa" é referente/sobre essa pessoa. E na maioria dos casos esta conexão é criada facilmente. Outro aspeto a considerar é que na relatividade deverá estar presente um destes elementos: "conteúdo", "finalidade" ou "resultado" (GT29, p. 10).
c) "Identificada ou Identificável", (GT29, p. 13)	A pessoa pode ser declarada como "identificada" quando é diferenciada dentro de um grupo. Este reconhecimento é alcançado através de informações que distinguem e que têm uma conexão privilegiada e próxima com a pessoa em causa.
d) "Pessoa singular", (GT29, p. 23)	Esta salvaguarda destina-se a pessoas singulares, logo, é possível afirmar que o direito à proteção dos dados pessoais é universal e não se restringe a nacionais ou a pessoas residentes num determinado país. "os sistemas de tratamento de dados estão ao serviço do Homem" e estes "devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência." (Consideração 2, D95). "Todos são iguais perante a lei e, sem distinção, têm direito a igual protecção da lei. Todos têm direito a protecção igual contra qualquer discriminação que viole a presente Declaração e contra qualquer incitamento a tal discriminação." (art.º 7, DUDH)

Fonte: Elaboração própria, com base no Parecer nº 4/2007, do GT29.

Ao analisamos a lei portuguesa de adaptação do RGPD (Lei n.º 58/2019), já não se definem os termos, mas sim desenvolve-se a proteção no tratamento dos dados pessoais, nestas instâncias.

Nos dias de hoje as Tecnologias da Informação e de Comunicação (TIC) têm um papel extremamente importante, visto permitirem um fluxo de informação e métodos de trabalho mais autónomos o que, por conseguinte, propenso a gerar conflitos. O tratamento de dados pessoais que temos vindo a expor até ao momento, vem possibilitar definir o perfil pessoal: nome, email, morada, preferências, caráter, comportamento, atitudes, entre outros. Em boa verdade esta recolha de informação pode ser aproveitada não apenas para fins promocionais (marketing), mas também na conjuntura laboral. Este sistema de agregação é a base da inteligência artificial e algoritmos e o uso

impróprio destas ferramentas TIC, em consequência pode lesar a vida privada dos titulares dos dados (vida profissional e extraprofissional), logo dados laborais também recaem nesta categoria (Moreira, 2017). Sendo assim, questões de trabalho como o grau de subordinação, por exemplo, podem inferir negativamente o individuo na sua esfera privada.

Uma das áreas setoriais mais sensíveis da nossa disposição jurídica é o Direito do Trabalho, no que respeita as alterações tecnológicas exponenciais e a sua interferência. Pelo que, num contexto de mudanças constantes torna-se imperativo adaptar estruturalmente e em termos funcionais, a complexidade do sistema laboral (Moreira, 2017).

Ao procurarmos os departamentos empresariais que recolhem, tratam, processam e armazenam a maior parte dos dados pessoais, por conseguinte temos os recursos humanos (RH), jurídicos e os financeiros (por exemplo), como os mais imbuídos pelo RGPD, embora este é transversal a todas as áreas. Facto transversal a todas as organizações independente do tamanho ou natureza (pública ou privada), que se encontram obrigadas a estar em conformidade com o RGPD, enfrentando assim várias complexidades inerentes.

A complexidade no caso da gestão de recursos humanos (GRH), impõe a necessidade de remodelação das funcionalidades, por exemplo, embora a informação respeitante à segurança e saúde no trabalho estarem afetas ao indivíduo, ambas necessitam de uma separação lógica, já que temos benefícios de informação sobre assiduidade, mas há também o direito ao esquecimento. A organização precisa assim, encontrar um equilíbrio para navegar a gestão de tratamento de dados pessoais, entre as suas obrigações e os direitos dos seus trabalhadores, ambos afetos no RGPD e no Código de Trabalho (CT).

O RGPD ao apresentar-se transversal a todas as áreas de uma organização acarreta a “criação e adoção de procedimentos, documentos e condutas internas” (Pais, 2021), com o intuito de proteger os dados pessoais e minorar a presença de violações de dados.

Sem esquecer que “o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho (CT) e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo.”, segundo o nº1 do art.º.28 da Lei n.º 58/2019. Expomos, de seguida, algumas das suas especificações (quadro 6).

Quadro 6: Comparação entre RGPD, CT e CC – Proteção dos dados dos trabalhadores

RGPD	CT	Conclusões
"…tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade". Todavia, realça ainda que "…respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais …o direito à ação e a um tribunal imparcial…" (Consideração 4, (UE) 2016/679).	"O empregador não pode exigir a **candidato a empreg**o ou a **trabalhador** que preste informações relativas: a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação" (art. º17, nº1, a), CT).	À entidade patronal é proibido exigir ao individuo qualquer elemento informativo da sua vida privada. A não ser que esta seja indispensável para o desenvolvimento da ocupação em causa e/ou para qualificar a sua aptidão para a realização da mesma.
"Deverão ser considerados dados pessoais relativos à **saúde** todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro…e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro" (Consideração 35, (UE) 2016/679).	"À sua **saúde ou estado de gravidez**, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação." (art.º 17, nº1, b), CT). "As informações previstas … são prestadas a **médico**, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a actividade." (art.º 17, nº2, CT).	Estas informações com o referencial de saúde são concedidas apenas a um **médico**, que informa a entidade patronal se o individuo está ou não apto, para desempenhar a atividade em questão.
Código Civil: "Todos devem guardar reserva quanto à **intimidade da vida privada** de outrem" (art.º 80, nº1, Código Civil (CC)).	"O empregador e o trabalhador devem respeitar os **direitos de personalidade** da contraparte, cabendo-lhes (…) O **direito à reserva da intimidade da vida**	Tanto CC como o CT, reservam o respeito mútuo do direito à intimidade da vida privada dos constituintes desta relação

	privada abrange quer o acesso, quer a divulgação de aspectos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afectiva e sexual, com o estado de saúde …" (art.º 16, nº1 e 2, CT).	(entidade patronal e individuo trabalhador). Por outro lado, o CT eleva ainda esta ligação, com o direito de personalidade.

Fonte: Elaboração própria.

O art.º 17º do CT torna-se assim a norma a seguir, em todas os ações e negociações jurídicas que incluam os preâmbulos da constituição do contrato de trabalho.

Outra questão importante é o facto de ao existir subordinação jurídica da relação laboral, subsiste um risco maior de incumprimento no tratamento de dados pessoais, por parte da instituição laboral, do que do oposto, já que este tratamento é analítico, logo desprovido de sensibilidade. O que torna ainda mais premente a tutela do direito de personalidade e privacidade do individuo trabalhador.

Neste sentido a instituição laboral pode instituir regras de uso de meios de comunicação (entre outros), pela imposição de limites (art.º 22, n.º 2, CT), sendo que estas regras devem sobrevestir a forma de normas internas, adequadas e proporcionais (art.º 22, n.º 1, CT), tendo também em conta as disposições do RGPD.

Tendo já sido analisados os conceitos: dados pessoais e tratamento, segundo a D95 e ao RGPD, desenvolveremos agora a continuação da exploração das influências ao sistema normativo português, face a estas questões.

O quadro 7 explicita o desenvolvimento dos seguintes conceitos: o Direito à vida privada, a Proteção de pessoas singulares, o Direito à proteção da vida privada, os Princípios da proteção de dados e o incentivo à Pseudonimização.

Quadro 7: Conceitos: Direito à vida privada, Proteção pessoas singulares, Direito à proteção da vida privada, Princípios da proteção de dados e o incentivo à Pseudonimização

Norma / Regime jurídico	Contexto e Considerações:
"A todos são reconhecidos os **direitos à identidade pessoal**, ao desenvolvimento da personalidade, à capacidade civil, à cidadania,	A CRP e o Tribunal Constitucional através destes três artigos delineiam o **direito à vida privada** para

ao bom nome e reputação, à imagem, à palavra, à reserva da **intimidade da vida privada** e familiar e à protecção legal contra quaisquer formas de discriminação" (art.º 26, nº1, CRP). "Todos os cidadãos têm o **direito de acesso aos dados informatizados** que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o **direito de conhecer a finalidade** a que se destinam, nos termos da lei." (art.º 35, nº1, CRP). "O direito à reserva da intimidade da vida privada e familiar também não é violado pela norma sub iudicio. 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. (…) direito a uma esfera própria inviolável, onde ninguém deve poder penetrar sem autorização do respectivo titular — compreende: a) a **autonomia**, ou seja, o direito a ser o próprio a regular, livre de ingerências estatais e sociais, essa esfera de intimidade; b) o **direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do interessado**" (nº13, Acórdão nº 128/92). "Todos devem guardar **reserva quanto à intimidade da vida privada de outrem**." E a "extensão da reserva é definida conforme a natureza do caso e a condição das pessoas." (art.º 80, nº1 e 2, CC). **"**Qualquer pessoa tem **direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência**. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros." (art.º 8, nº1 e 2, Convenção Europeia dos Direitos Humanos). "Todas as pessoas têm **direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações**." (art.º 8, nº1 e 2, CDFUE).	todos e **direito de conhecer a finalidade dos seus dados informatizados**. Estabelece o direito a uma **esfera própria inviolável**, **onde ninguém deve poder penetrar sem autorização do respetivo titular.** Bem como, **direito ao seu domicílio, pelas suas comunicações e correspondências.**
"A **proteção** conferida pelo presente regulamento deverá aplicar-se às **pessoas singulares**, **independentemente da sua nacionalidade** ou do seu local de **residência**, relativamente ao **tratamento dos seus dados pessoais**. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas	Relembramos que os dados pessoais caraterizam-se por serem todas as informações sobre um individuo singular, que permita identificação (direta ou indiretamente) sobre a sua vida (privada ou profissional). Estes dados não são apenas números

coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva." (consideração 14, RGPG - (UE) 2016/679)	de segurança social, mas também elementos profissionais ou de outro carisma (por exemplo: dados genéticos ou biométricos). Pelo que esta lei confere a **proteção no tratamento de dados pessoais às pessoas singulares, independentemente da nacionalidade ou do seu local de residência.**
"Ninguém sofrerá intromissões arbitrárias na **sua vida privada**, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem **direito a protecção** da lei" (art.º 12, DUDH).	O **direito à proteção de dados pessoais** surge através de um dos direitos fundamentais do ser humano, reconhecido na Declaração Universal dos Direitos do Homem (DUDH) (Diário da República Eletrónico, 2021), ou seja, o **direito à proteção da vida privada**. Os dados pessoais dispõem assim de informações sobre a vida privada, logo, a sua salvaguarda deve ser corretamente garantida. Nota: A DUDH foi adotada e proclamada em 1948, pela Assembleia Geral e publicada no Diário da República, I Série A, n.º 57/78.
"A fim de se evitar o sério risco sério de ser contornada a **proteção das pessoas singulares**, esta deverá ser **neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas**. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por **meios automatizados**, bem como ao **tratamento manual**, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento." (consideração 15, RGPG - (UE) 2016/679)	Saliente-se ainda que a **proteção de dados das pessoas singulares** deve ser **neutra em termos tecnológicos** e **independentemente das técnicas usadas** (tratamento automatizado ou manual).
"Os **princípios da proteção de dados** deverão **aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável**. Os dados pessoais que tenham sido **pseudonimizados**, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados **informações sobre uma pessoa singular identificável**. Para determinar se uma pessoa singular é identificável, importa considerar todos os **meios suscetíveis de ser razoavelmente utilizados**, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para	De acordo com o considerado neste artigo é reiterado pelos **princípios de proteção de dados, todos os dados pessoais**, mesmo que tenham sido pseudonimizados, mas que **possam ser identificáveis por meio de informações adicionais**. É importante equacionar todos os **meios suscetíveis** de acessibilidade e **razoáveis de serem utilizados** e para o determinar é importante equacionar fatores como: custos e o tempo necessário para a identificação, face a tecnologia

identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a **evolução tecnológica**…" (Consideração 26, RGPD - (UE) 2016/679)	disponível de tratamento dos dados e a evolução tecnológica.
"O presente regulamento **não se aplica aos dados pessoais de pessoas falecidas**. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas." (Consideração 27, RGPG - (UE) 2016/679)	O regulamento **não é extensível aos dados pessoais de pessoas falecidas**.
"A fim de criar **incentivos** para **aplicar a pseudonimização** durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento." (Consideração 29, RGPG - (UE) 2016/679). "As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão () ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares." (Consideração 30, RGPG - (UE) 2016/679)	Estes 2 artigos têm a finalidade de gerar estímulos para o **emprego da pseudonimização na duração de tratamento de dados pessoais**. Importa garantir que o **responsável** pela aplicação destas medidas possa: 1) fazer uma análise geral do tratamento quando tiver tomado as **medidas técnicas e organizativas** necessárias para assegurar o tratamento em questão, 2) garantindo a **aplicação deste regulamento** e 3) a **conservação em separado** das informações adicionais que possibilitam associar os dados pessoais a um titular de dados específico. E 4) **identificar** também as pessoas autorizadas a aceder a cada repartição de informação. Rematamos com a necessidade de aluir que as pessoas singulares podem ser relacionadas com vários dados, como por exemplo: aplicações, ferramentas e protocolos. E estes identificadores podem ser considerados de informações adicionais.

Fonte: Elaboração própria.

Após o desenvolvimento destes conceitos, sentimos a necessidade de abordar o tratamento de dados pessoais quanto às suas categorias especiais. Contextualizando o que já foi abordado até ao momento, apresentam-se no universo dos dados pessoais conceitos diversos associados, relembrando

que segundo a consideração 26 do RGPD, estes são designados como a "informação relativa a uma pessoa singular identificada ou identificável", isto é, o titular dos dados (Consideração 26, RGPG - (UE) 2016/679).

Pinheiro (2016, p. 374) mencionou que este conceito "abrange uma pluralidade de informação pessoal que pode variar do nome à informação genética". No entanto, ele vai ainda mais longe e relembra que esta definição não se cinge apenas a determinados fatores como o nome, idade, entre outros, mas também a elementos como "dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocole* (IP), dados acadêmicos (...)" (Pinheiro, 2018, p. 26).

É fulcral que os dados pessoais sejam reconhecidos como um direito do indivíduo, sendo necessária a sua salvaguarda, impondo-se o direito ao consentimento e autodeterminação. Vaz (2018) também alega que este conceito é deveras lato e que para além de abranger dados, como os mencionados inicialmente – dados de localização e IP – existem os metadados e os *big data*.

Machado, por seu lado descreve que os dados pessoais se representam por "todas as informações relativas a uma pessoa singular viva identificada ou identificável, quer sejam dados relacionados com a vida pessoal, profissional ou pública. Incluem-se também todos os conjuntos de dados distintos que permitem a identificação de uma pessoa" (2020, p. 20).

Posto isto, o RGPD ((UE) 2016/679) determina que os dados podem apresentar categorias especiais (art.º 9, nº1) e que estas ganham pertinência de tratamento pela sua natureza, logo requerem um cuidado especial. Temos, então, as seguintes categorias especiais de dados pessoais (art.º 9, nº1, RGPD):

Figura 2: Categorias especiais de dados pessoais

Categorias Especiais de Dados Pessoais

- a origem racial ou étnica;
- as opiniões políticas;
- as convicções religiosas
- as convicções filosóficas;
- a filiação sindical;
- os dados genéticos;
- os dados biométricos para identificar uma pessoa de forma inequívoca;
- os dados relativos à saúde;
- os dados relativos à vida sexual ou orientação sexual de uma pessoa.

Fonte: art.º 9, nº1, RGPD - (UE) 2016/679.

Estes são dados que podem colocar em causa os direitos e liberdades fundamentais dos indivíduos, dependendo do contexto em que são tratados e por norma é proibido este tratamento, exceto quando previsto por disposição legal (art.º 9, nº2 e 3, RGPD).

Sendo assim, existem exceções nas situações em que é facultado o consentimento explícito (art.º 9, nº2, a), RGPD), necessidade para matérias laborais, judiciais, interesse público, saúde pública, medicina no trabalho (art.º 9, nº2, b) a j), RGPD). Ainda existe legitimidade de tratamento quando, o titular tenha manifestado explicitamente e publicamente esses dados (Consideração 154, RGPD). Por todos estes argumentos de complexidade de tratamento, garantem que estes ficam subordinados a circunstâncias de tratamento específicas.

Analisando a Lei n.º 58/2019, através do art.º 23, nº1 consentir o tratamento de dados pessoais com natureza excecional, isto é, estando neste tratamento assim abrangidas as entidades públicas para aplicações distintas das definidas pela recolha, facto que deve ser convenientemente justificado, por forma a certificar a prossecução do interesse público, que de outra forma não possa ser acautelado.

Francisco e Francisco (2019, p. 29) interpretam assim, que "o teste decisivo para decidir se são dados pessoais para o RGPD ou não, consiste em avaliar se esses dados podem ser usados direta ou indiretamente para identificar uma pessoa".

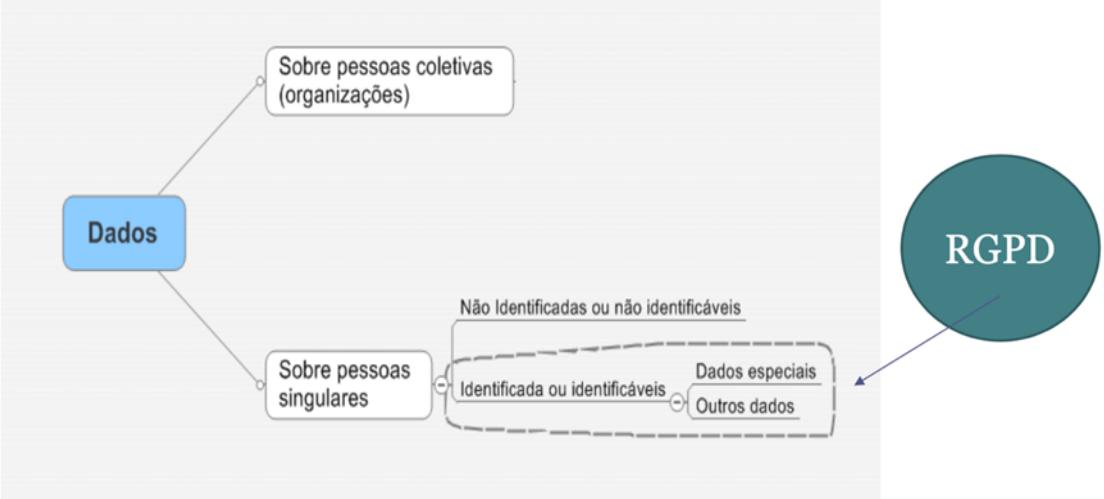
O tratamento destes dados é referido por Penteado (2018, p. 8) como uma "operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados". Para executar este tratamento é necessário primeiramente, contextualizar os respetivos dados que fazem parte do processo de negócio (Lourenço, Penteado e Gago, 2018).

Dionísio (2018, p. 37) por outro lado, recorda que "para que haja um tratamento lícito desses dados é necessário que o titular dos dados conceda uma autorização para esse tratamento, ou seja que dê o consentimento, sendo que este deverá ser expresso e obtido de forma lícita".

Em termos práticos, como exemplos de operações para o tratamento de dados, de acordo com a Secretaria-Geral da Presidência do Conselho de Ministros (2018), temos o processamento salarial e a gestão do pessoal, a destruição de documentos que contenham dados pessoais, a colocação de fotografias pessoais em *websites*, entre outros.

Em síntese, de forma a compreendermos o âmbito de aplicação do RGPD, Penteado (2018), apresenta-nos a esquematização seguinte.

Figura 3: Aplicação do RGPD



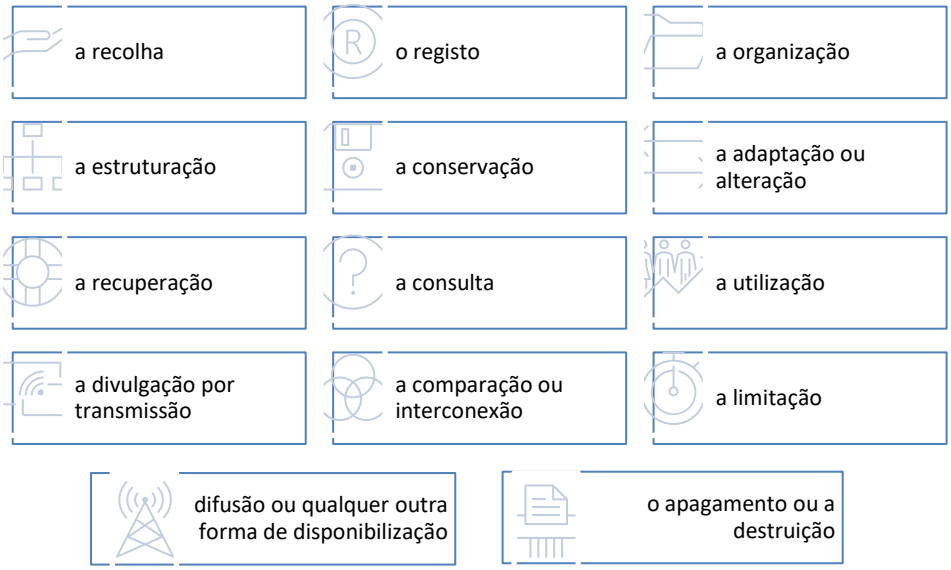
Fonte: Penteado (2018).

Esta figura deixa subjacente a ideia de que se um tratamento de dados específico (automatizado ou não) possibilita a identificação do seu titular dentro de um todo (grupo), então este processo fica sujeito ao RGPD.

2.2 FORMAS DE TRATAMENTO DE DADOS PESSOAIS

Apresenta-se de seguida a lista das formas de tratamento dos dados pessoais, que se encontram explicitas no art.º 4, nº2 do RGPD (UE) 2016/679).

Figura 4: Formas de tratamento dos dados pessoais



Fonte: art.º 4, nº 2 do RGPD - (UE) 2016/679.

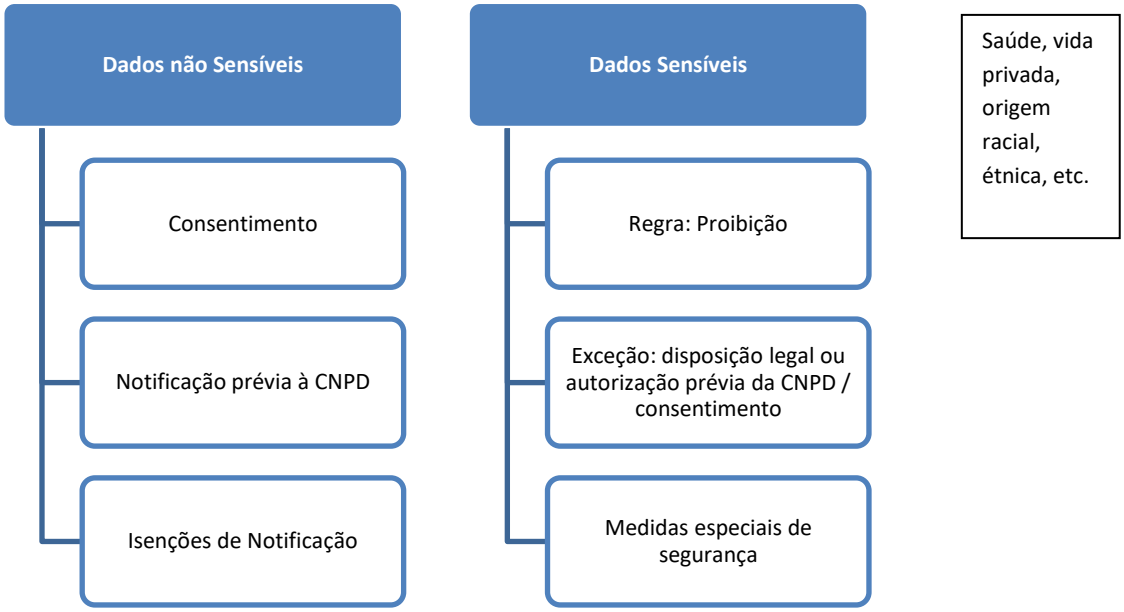
Nesta lista constam todos os exemplos de operações que podem ser realizadas com ou sem recursos automatizados.

Machado relembra uma operação que acresce a esta lista (2020, p. 21) já que refere também a: Retificação, suplantada pelo art.º 16, RGPD - (UE) 2016/679. E por forma a dar alguma palpabilidade a esta questão, Machado avança igualmente, com um rol de tipos de dados pessoais, que podem ser tratados dentro do contexto empresarial (2020, p. 22):

- "Dados de recrutamento;
- Dados do pessoal;
- Dados de clientes;
- Dados de parceiros (fornecedores/prestadores de serviços);
- Dados pessoais de utilizadores de websites".

Resta nesta fase perceber quais os primeiros passos no tratamento de dados pessoais e o que isso acarreta, que diferentes áreas, direitos e deveres. O que equacionar antes de principiarmos o tratamento dos dados? Bem como, a questão dos dados de caraterística especial?

Figura 5: O que fazer antes de dar início ao tratamento de dados?

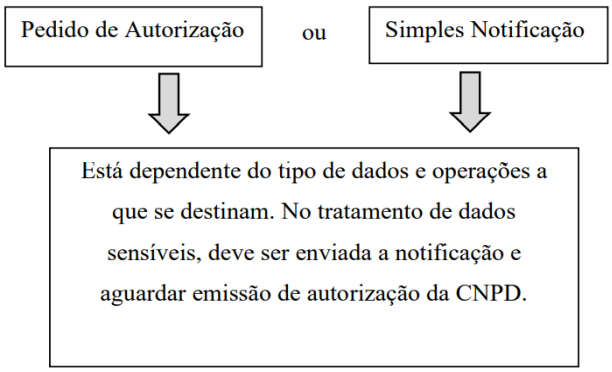


Fonte: Adaptado de APDSI (2014).

Machado (2020) relembra que primeiro é importante classificar os dados, pois por norma quando estão afetos dados especiais ou sensíveis é ilícito o seu tratamento, em detrimento das suas exceções.

Segundo a APDSI (2014) este processo de tratamento começa com o pedido de consentimento ao titular desses dados (pessoa a quem os dados dizem respeito), exceto nos termos dispensados por lei.

Figura 6: Autorização/Notificação CNPD



Fonte: Adaptado de Machado (2020).

O segundo tramite passa por uma notificação ou requerimento de autorização do tratamento à CNPD (dependendo dos casos): etapa indispensável para qualquer organização, que a partir desse momento se torna responsável pelo tratamento de dados pessoais.

Existem quatro constituintes que assumem responsabilidade no que se refere ao tratamento de dados, de acordo com o Magalhães (2018, p. 10) e Dionísio (2018, p. 47):

- **Responsável pelo tratamento**: pessoa singular/coletiva ou entidade que estabelece o destino e quais os meios de tratamento de dados pessoais;
- **Subcontratante**: pessoa singular/coletiva ou entidade que irá atuar sob os dados pessoais, por conta do responsável definido pelo tratamento destes;
- **Destinatário**: pessoa singular/coletiva ou entidade que obtém comunicações sobre dados pessoais;
- **Terceiro**: pessoa singular/coletiva ou entidade que não seja o possuidor dos dados.

Dissecando o RGPD através da Lei n.º 59/2019, desenvolvemos, seguidamente, os princípios indispensáveis para o tratamento de dados pessoais (quadro 8):

Quadro 8: Princípios indispensáveis no tratamento de dados pessoais

Princípio	RGPD através da Lei n.º 59/2019
Princípio da licitude e da lealdade	Reitera que os dados pessoais são "objeto de um tratamento lícito e leal" (art.º 4, n.º 2, a), RGPD).
Princípio da limitação das finalidades	"Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados de forma incompatível com essas finalidades" (art.º 4, n.º 2, b), RGPD).
Princípio da minimização dos dados	"Adequados, pertinentes e limitados ao mínimo necessário à prossecução das finalidades para as quais são tratados" (art.º 4, n.º 2, c), RGPD).
Princípio da exatidão	"Exatos e atualizados sempre que necessário, devendo ser tomadas todas as medidas razoáveis para que os dados inexatos sejam apagados ou retificados sem demora" (art.º 4, n.º 2, d), RGPD).
Princípio da limitação da conservação	"Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados" (art.º 4, n.º 2, e), RGPD).
Princípio da integridade e confidencialidade	"Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas" (art.º 4, n.º 2, f), RGPD).
Princípio da responsabilidade	O responsável pelo tratamento necessita de anuir as "medidas que lhe permitam comprovar que o tratamento de dados pessoais é realizado em conformidade com os princípios enunciados no número anterior" (art.º 4, n.º 3, RGPD). Esta lei define, ainda, o responsável pelo tratamento como a "entidade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais, ou, no caso em que estes são determinados por lei, a autoridade nela indicada" (art.º 3, n.º 1, j), RGPD). E o subcontratante como a "pessoa singular ou coletiva, a autoridade pública, o serviço ou outro organismo que trata dados pessoais por conta do responsável pelo tratamento" (art.º 3, n.º 1, k), RGPD).
Princípio do consentimento	Este princípio encontra-se imiscuído nesta Lei em diferentes frentes, maioritariamente advertindo a necessidade de consentimento, como por exemplo: "…dados pessoais tratados ao abrigo da presente lei, sem previsão legal ou consentimento, é punido…" (art.º 54, nº1); "…sem o devido consentimento, revelar ou divulgar, no todo ou em parte, dados pessoais tratados ao abrigo da presente lei, é punido…" (art.º 58, nº1). Já o ato positivo é quando "os dados pessoais não são disponibilizados a um número indeterminado de pessoas sem o consentimento do respetivo titular dos dados" (art.º 21, nº 3, RGPD).

Fonte: Elaboração própria, segundo o RGPD através da Lei n.º 59/2019.

Neste contexto Machado (2020) simplifica a questão do princípio de licitude (ver próxima Figura), listando os requisitos que podem tornar o tratamento de dados lícito.

Para o tratamento dos dados considerar-se lícito tem de apresentar um destes requisitos: "Há consentimento da parte do titular dos dados; Execução de diligências pré-contratuais ou do próprio

contrato; Cumprimento de uma obrigação jurídica; Este tratamento seja em virtude da defesa dos direitos e interesses vitais do titular dos dados; Exercido por uma autoridade pública ou no exercício de funções de interesse público ou Sempre que necessário desde que os interesses do responsável sejam legítimos, desde que não prevaleçam os interesses do titular" (Machado, 2020, p. 23 e art.º 6, nº 1, (UE) 2016/679).

2.3 DIREITOS DOS TITULARES DE DADOS E CONSENTIMENTO

Neste ponto procede-se à análise do conjunto de direitos que salvaguardam os dados pessoais dos titulares, do interveniente que procede ao seu tratamento (responsável).

Quadro 9: Direitos dos Titulares

Direito	Norma: RGPD - (UE) 2016/679
Direito à informação clara Ao titular dos dados subsiste o direito à informação de como é que estes são usados, subsistindo uma forma clara, transparente e facilmente compreensível (nº1, art.º 14, RGPD).	"Quando os dados pessoais forem recolhidos junto do titular, o **responsável pelo tratamento faculta-lhe**, aquando da recolha desses dados pessoais, as seguintes informações: a) A **identidade** e os contactos do **responsável** pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As **finalidades** do tratamento a que os dados pessoais se destinam, bem como o **fundamento jurídico** para o tratamento; d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; e) Os **destinatários** ou categorias de destinatários dos dados pessoais, se os houver." (art.º 13, RGPD)
Direito de Acesso Ao titular dos dados assiste o direito de obter do responsável a confirmação se os dados pessoais são ou não objeto de tratamento e em caso afirmativo, o direito de aceder e obter informação sobre os seus dados pessoais que são tratados.	"1. O titular dos dados tem o direito de obter do responsável pelo tratamento a **confirmação** de que os dados pessoais que lhe digam respeito **são ou não objeto de tratamento** e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As **finalidades** do tratamento dos dados; b) As **categorias** dos dados pessoais em questão; c) Os **destinatários** ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o **prazo previsto de conservação** dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a **retificação**, o **apagamento ou** a **limitação** do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar **reclamação** a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a **origem** desses dados; h) A existência de **decisões automatizadas**, incluindo a definição de perfis, referida no artigo 22.o, nº 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem

	como a importância e as consequências previstas de tal tratamento para o titular dos dados." (art.º 15, nº1, RGPD)
Direito de retificação Ao titular dos dados persiste o direito de obter, a retificação ou atualização dos dados pessoais, quando eles não estão corretos.	"O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a **retificação dos dados pessoais inexatos** que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados **pessoais incompletos sejam completados**, incluindo por meio de uma declaração adicional." (art.º 16, RGPD).
Direito ao Apagamento dos Dados («direito a ser esquecido») Dá poderes ao titular dos dados para instar o seu apagamento ou eliminação, contando que não haja fundamentos válidos para o tratamento continuado, por parte do responsável. Este não se trata de um direito absoluto, logo admite exceções (por exemplo, defesa de um direito num processo judicial).	"O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais e este tem a **obrigação de apagar** os dados pessoais, quando se aplique um dos seguintes motivos: a) Os dados pessoais **deixaram de ser necessários para a finalidade** que motivou a sua recolha ou tratamento; b) O titular **retira o consentimento** em que se baseia o tratamento dos dados; c) O titular opõe-se ao tratamento e **não existem interesses legítimos** prevalecentes que justifiquem o tratamento; d) Os dados pessoais foram tratados **ilicitamente**; e) Os dados pessoais têm de ser apagados para o cumprimento de uma **obrigação jurídica** a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação." (art.º 17, nº 1, RGPD).
Direito à limitação do tratamento É concedido ao titular dos dados o direito de obter a limitação do tratamento, pelo responsável do tratamento.	"O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) Contestar a **exatidão dos dados pessoais**, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for **ilícito** e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para **efeitos de declaração, exercício ou defesa de um direito num processo judicial**; d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1 (direito de oposição), até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados." (art.º 18, nº 1, RGPD).
Direito à portabilidade dos dados Ao titular dos dados subsiste o direito de obter e reutilizar determinados dados pessoais, para novos assuntos próprios, bem como a sua partilha segura.	"O titular dos dados tem o **direito de receber** os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num **formato estruturado, de uso corrente e de leitura automática**, e o **direito de transmitir** esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir" (art.º 20, nº 1, RGPD).
Direito à oposição Ao titular dos dados é cedido o direito de se opor a determinados tipos de tratamento, por motivos particulares. Mas, o responsável pelo tratamento pode continuar a tratar esses dados se fizer prova de razões legítimas que se sobreponham aos interesses, direitos e liberdades do titular dos dados ou no caso de	"O titular dos dados tem o direito de se **opor a qualquer momento**, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, nº 1, alínea e) ou f), ou no artigo 6.o, nº 4, incluindo a definição de perfis com base nessas disposições. O **responsável** pelo tratamento **cessa o tratamento dos dados pessoais**, a **não ser que apresente razões imperiosas e legítimas** para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de

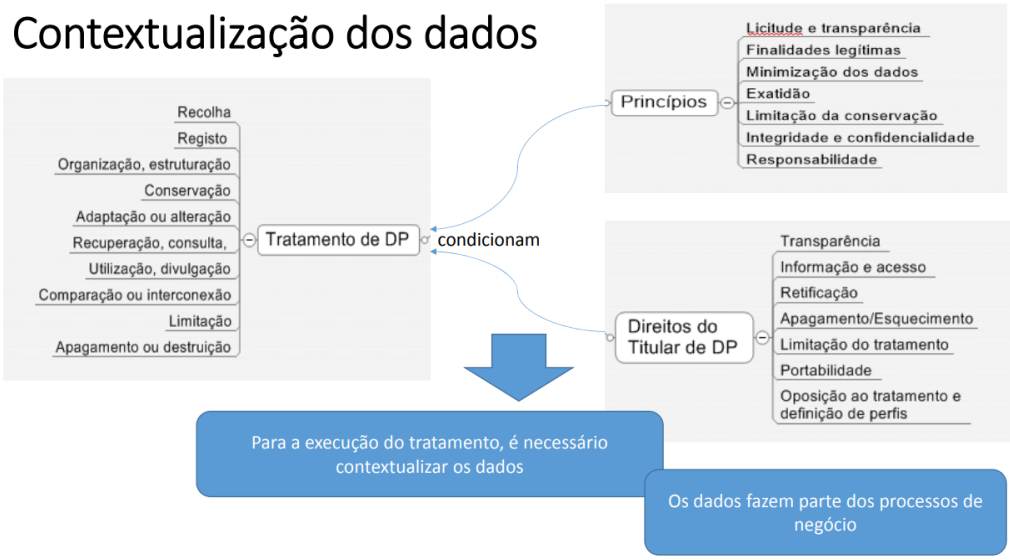
serem necessários o exercício ou a defesa de um direito num processo judicial.	declaração, exercício ou defesa de um direito num processo judicial." (art.º 21, RGPD).
Direito de retirar o consentimento É concedido ao titular dos dados o direito de vetar o consentimento a qualquer momento. Este deve ser tão fácil de ceder, como de retirar.	"O titular dos dados tem o direito de **retirar o seu consentimento a qualquer momento**. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento **deve ser tão fácil de retirar quanto de dar**." (art.º 7, nº3, RGPD).
Decisões individuais automatizadas, incluindo definição de perfis Ao titular dos dados é cedido o direito de não ficar "preso" ao perfil automatizado, principalmente se isso produzir efeitos na sua esfera jurídica.	"O titular dos dados tem o direito de **não ficar sujeito a nenhuma decisão** tomada exclusivamente com base no **tratamento automatizado**, incluindo a definição de perfis, que produza efeitos na sua **esfera jurídica** ou que o afete significativamente de forma similar." (art.º 21, nº1, RGPD). O nº 2 deste artigo abrange as exceções.
Direito de apresentar reclamação a uma autoridade de controlo Ao titular dos dados é facultado o direito de apresentar uma reclamação, se considerar que o tratamento dos seus dados pessoais viola o presente regulamento.	"Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm 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 presente regulamento." (art.º 77, nº1, RGPD).

Fonte: Elaboração própria, segundo o RGPD - (UE) 2016/679.

Uma novidade é o direito à portabilidade dos dados, que está intrinsecamente ligado ao direito de acesso. O seu grande cunho deve-se ao próprio propósito do direito à portabilidade dos dados e o facto do titular poder dar-lhes um novo uso e usufruir também de uma partilha segura. Também existe referência a este direito no artº 18 da Lei n.º 58/2019, em especial o nº 2 e 3, que reitera a importância de subsistir um formato que permita ao titular dos dados o seu acesso.

Depois de desenvolver os tipos de tratamento que os dados pessoais podem ser submetidos, os principios gerais subjacentes ao tratamento e os direitos do titular, importa igualmente analisar e perceber a importância da sua contextualização e o consentimento.

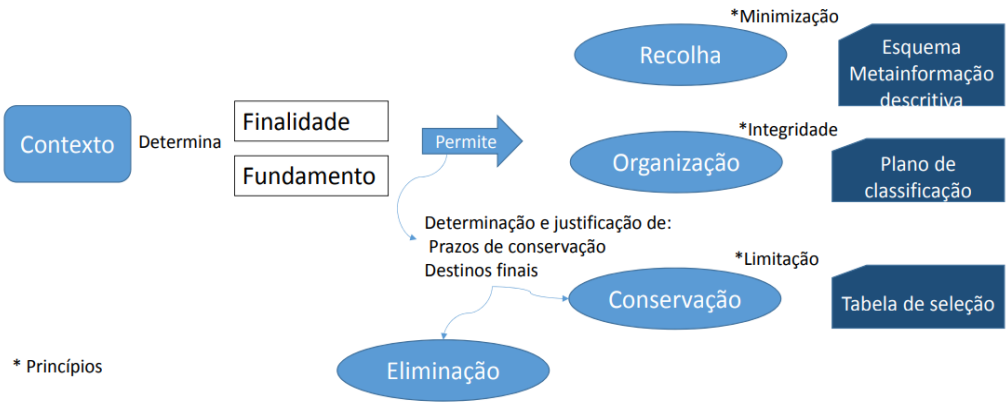
Figura 7: Contextualização dos dados



Fonte: Lourenço, Penteado & Gago (2018).

Com o auxílio deste esquema desenvolvido por Lourenço, Penteado e Gago (2018), percebemos que as formas de manuseamento dos dados particulares são condicionadas tanto pelos princípios, como pelos direitos dos titulares e, para o tratamento propriamente dito, é importante contextualizar os dados, sendo que os dados fazem parte dos processos de negócio.

Figura 8: Do contexto dos dados aos instrumentos de gestão de dados



Fonte: Lourenço, Penteado & Gago (2018).

Após a contextualização dos dados conforme é demonstrado na Figura 8, é importante determinar a finalidade e o fundamento da recolha. Depois chega o momento de avaliar se esta recolha é ou não licita, ou seja, permitida. Se esta é permitida procede-se à sua recolha propriamente dita, à sua organização, conservação ou eliminação, tendo em atenção os princípios de minimização, integridade e limitação, respetivamente por esta ordem. Neste ponto, existe uma adaptação dos instrumentos de gestão de dados dentro da organização, muito própria a cada caso. Estarão afetos a este processo as normas e esquemas de classificação e metainformação internos, por exemplo. No caso de a recolha não ser permitida a organização não tem acesso a estes dados, logo também não fica responsável por eles.

O consentimento é um dos pilares do RGPD, pelo que o seu pedido tem de ser apresentado de forma correta. Resumidamente, temos as seguintes caraterísticas que este pedido tem de cumprir: "forma clara e concisa, utilizando uma linguagem fácil de compreender, e de uma forma que o distinga claramente de outras informações, como os termos e condições. O pedido tem de especificar qual a utilização que será dada aos seus dados pessoais e tem de incluir os contactos da empresa que efetua o tratamento dos dados. O consentimento tem de ser dado de livre vontade e tem de ser específico e informado e de refletir os seus desejos de forma inequívoca." (Comissão Europeia (2021) e art.º 6 e 7, (UE) 2016/679).

Há que relembrar que houve necessidade de um período de adaptação, para que as entidades pudessem cumprir todos estes tramites legais, pelo que o consentimento teve especialmente de ser endereçado devido há sua importância. Antes deste período, o consentimento era obtido de forma tácita, isto é, abrangido nos termos e condições que excecionalmente era lido. “Isso deixa de ser válido.” (UC, 2021). Logo, é importante fazer esta transição e solicitar ao titular dos dados particulares um novo consentimento, ou seja, um novo consentimento informado, nas condições exigidas pelo RGPD. Sendo assim, a gestão de dados numa organização tem a prioridade de avaliar se os dados já reunidos na sua base de dados, preenchem os requisitos do consentimento necessário.

O consentimento informado é subentendido por “a autorização esclarecida prestada pelo utente antes da submissão a determinado ato…”. Este prevê ainda “uma explicação e respetiva compreensão quanto ao que se pretende fazer, o modo de atuar, razão e resultado esperado da intervenção consentida” (Portal dos Serviços Públicos, 2021).

O consentimento informado implica assim, que ao titular dos dados têm de ser facultadas pelo menos, estas informações sobre o tratamento:

1. a identidade da organização que efetua o tratamento dos dados;
2. os fins para os quais os dados estão a ser tratados;

3. o tipo de dados que serão tratados;
4. a possibilidade de retirar o consentimento dado (por exemplo, enviando uma mensagem de correio eletrónico para retirar o consentimento);
5. se aplicável, o facto de os dados serem utilizados para decisões exclusivamente automatizadas, incluindo a definição de perfis;
6. informações destinadas a apurar se o consentimento está relacionado com uma transferência internacional dos dados, os possíveis riscos de transferências de dados para fora da UE se tais países não estiverem sujeitos a uma decisão de adequação da Comissão e não existirem garantias adequadas, (Comissão Europeia, 2021).

Deixamos, ainda, a nota de que este novo consentimento informado, nada tem a ver com a Renovação de Consentimento do art.º 61, da Lei nº 58/2019**.**

3. PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA E GESTÃO DOCUMENTAL

3.1 RGPD E ADMINISTRAÇÃO PÚBLICA

Com as tecnologias digitais advém novas formas de comunicação, sendo que desta forma é possível um acesso e recuperação de informação rápido e facilitado (Grisoto et al., 2015). Qualquer indivíduo é perfeitamente capaz de aceder neste meio digital a informações, tendo em conta que não existe uma barreira geográfica e o fluxo de informação é intenso (Pinto, 2018). "A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais". E, a "recolha e a partilha de dados pessoais registaram um aumento significativo" (Consideração 6, (UE) 2016/679).

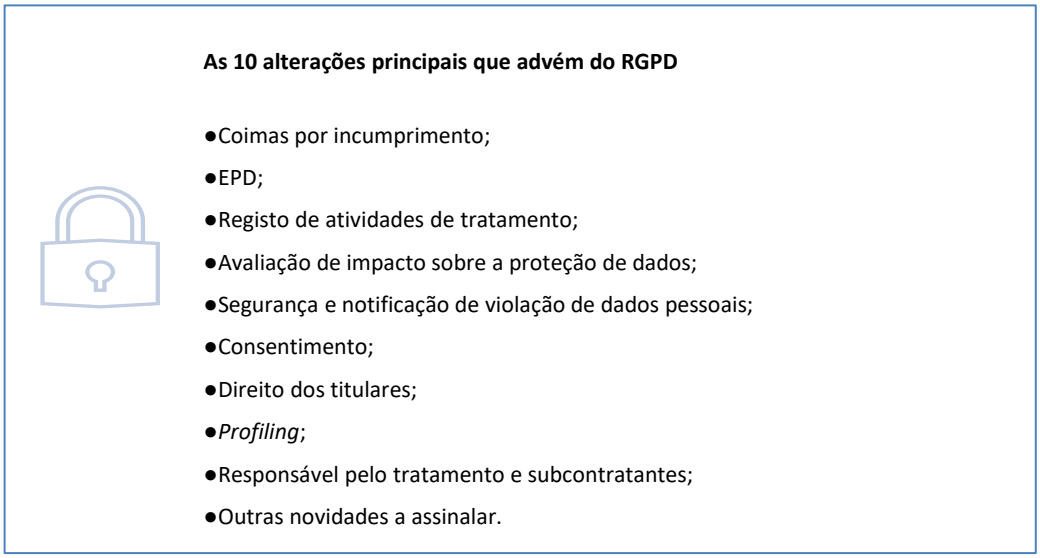
De acordo com este regulamento, o digital veio proporcionar às entidades públicas uma utilização de dados sem precedentes nos exercícios das atividades, já que os titulares disponibilizam publicamente e de forma global, cada vez mais os seus dados particulares. A economia e a vida social sofreram um grande impacto pelas tecnologias, mas contribuirão para "facilitar a livre circulação de dados pessoais na União Europeia e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais" (Consideração 6, (UE) 2016/679).

Desta forma, "o aumento da eficiência nos métodos de monitoramento e investigação proporciona maior facilidade para manter, utilizar e coletar informações" (Finkelstein & Finkelstein, 2019, p. 288).

O RGPD "tem como objetivo principal harmonizar as leis de privacidade de dados no bloco europeu, regulando o processamento por indivíduos, empresas ou organizações de dados pessoais relacionados a indivíduos do bloco" (Iramina, 2020, p. 94). E vem viabilizar a liberdade e a segurança aos indivíduos, sendo que com este regulamento "houve uma normalização do que seriam os atributos para proteger esses direitos fundamentais, fazendo com que surjam regulamentações com essa mesma linha de pensamento à medida que trazem instrumentos para controlar as relações derivadas dessa era digital" (Freitas, 2020, p. 9)

O impacto deste regulamento nas organizações provoca inúmeras alterações em diferentes graus organizacionais, conforme se tem vindo a expor, mas para existir sucesso nesta implementação é necessário subsistir uma boa gestão na mudança organizacional (Coreni, 2018).

Figura 9: Principais alterações que advêm do RGPD



Fonte: Fazendeiro (2017).

Esta figura apresenta a lista das dez alterações principais que advém do RGPD, segundo Fazendeiro (2017).

Por outro lado, em termos práticos uma organização nos dias de hoje, não pode negligenciar da importância da proteção de dados, na gestão de documentos. Para que esta realidade seja conseguida numa organização, segundo a empresa *DocuSign* (2021), uma boa administração de documentos, deve garantir estas oito vertentes:

1. Acompanhamento tecnológico (privilegiar a adaptação, com os recursos tecnológicos mais recentes);
2. Acesso discriminado aos documentos (difícil equilíbrio entre critérios de segurança eficientes, face a implementação de mecanismos de acesso facilitado, a quem requer a informação);
3. Digitalização (manipulação, armazenamento e partilha são mais céleres e simples);
4. Ferramentas de segurança da informação (adoção de recursos, como a criptografia e controlo de acessos, através de credenciais e senhas);
5. Manutenção de cópias de segurança (manter atualizada as cópias de segurança dos arquivos que vão sendo digitalizados, garantindo um backup fidedigno à data);
6. Não desvalorizar a importância dos documentos (manter a documentação acessível pelo tempo indispensável; por exemplo, há provas fiscais que é obrigatório preservar, por um período de tempo);
7. Assinatura eletrónica (este recurso agilizará determinados processos) e
8. Alinhamento na política de GD (o investimento na automação de processos e tecnologias deve-se repercutir em metodologias concomitantes).

Relembramos que por um lado temos o regulamento (UE) 2016/679 e por outro a CRP, onde ambos determinam a proibição de acesso a dados pessoais de terceiros, como regra geral. Ao equacionar o direito do cidadão de ser informado e ter acesso à atuação administrativa, então já existe a salvaguarda dos princípios orientadores da atividade administrativa na disposição jurídica portuguesa (princípio da informação, transparência administrativa e da administração aberta). Apresenta-se neste plano uma necessidade de correlação deste novo paradigma, uma vez que o RGPD não tem objetivos de desrespeitar os princípios diretores da atividade administrativa ou interditar o acesso do cidadão aos documentos administrativos.

As funções da AP resultam da relação permanente existente, com o Estado e a Sociedade (Pereira, 2018). Sendo estas funções exercidas no âmbito de cargos executivos, legislativos ou judiciários. Esta relação tem como interesse a melhoria da qualidade da gestão pública. Segundo Tavares a AP é "o poder de gestão do Estado, que se manifesta no poder de regulamentação, tributar e fiscalizar, através dos seus órgãos e outras instituições", tendo sempre como foco a "prossecução do serviço público" (2019, p. 7). Além disso, a atividade da AP é "desenvolvida por um conjunto de entidades, pessoas coletivas de direito público, integradas por um vasto conjunto de serviços públicos, especificadamente instituídos para o efeito" (Almeida, 2015 p. 16).

A AP encontra-se sujeita às regras do RGPD, "no âmbito das suas competências e atribuições conferidas por lei aos serviços públicos", tendo a "legitimidade para tratar dados pessoais dos administrandos, devendo esse tratamento ser pautado pelos princípios fundamentais de tratamento de dados pessoais consagrados no RGPD", particularmente "tratamento equitativo e lícito, limitação da finalidade, minimização dos dados e conservação dos dados" (Teves, 2019, p. 101).

Francisco e Francisco (2019) referem ainda que a AP por estar legitimada para consumar o tratamento dos respetivos dados pessoais, terá na mesma que aplicar os princípios do RGPD (art.º 5, (UE) 2016/679), garantindo desta forma, o cumprimento das finalidades determinadas. Embora, no caso de um tratamento que esteja para além das suas competências, é necessário que a AP confirme a necessidade de associar outros meios de licitude, como por exemplo o consentimento do titular dos dados.

Neste contexto, o tratamento deve ser devidamente fundamentado, com objetivos de interesse público que de outra forma não possa ser salvaguardado, o artigo 26 da Lei n.º 58/2019, concede casos excecionais. Segundo este pressuposto, garante ainda a autorização de transmissão destes dados pessoais entre entidades públicas (ou seja, com motivos dispares dos definidos na recolha) e sendo necessário este tratamento fazer parte de um protocolo, que demarque as responsabilidades de cada entidade mediadora.

Esta implementação do regulamento no contexto da AP, vem decretar que toda a organização seja envolvida nestas mudanças, necessitando de um maior conhecimento, de forma a facilitar a identificação dos respetivos dados pessoais que têm que ser tratados, em que tipo de processos se sucedem, os tratamentos e se estes tratamentos estão enquadrados com os estabelecidos no RGPD.

De acordo com o analisado e segundo Teves (2019), esta implementação precisará de incluir três conjuntos de atividades, particularmente os:

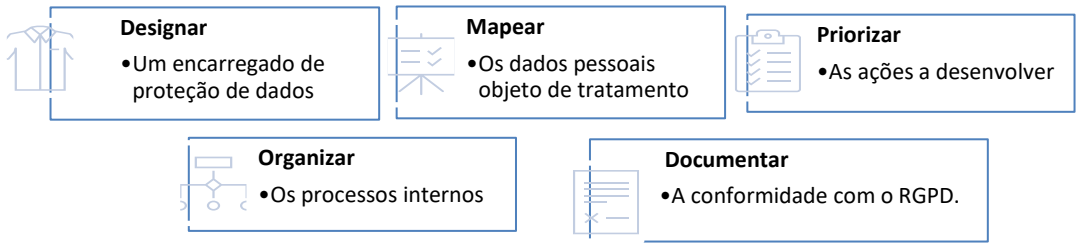
- **Recursos Humanos**: formação profissional e sensibilização dos RH;
- **Processo**: auditorias, implementação de melhores práticas e gestão de sistemas e dados pessoais;
- **Tecnologia**.

Denota-se que é um processo longo e árduo que a AP tem de prosseguir e sustentar, incluindo uma extensa análise e estudo dos procedimentos relativos ao tratamento de dados pessoais. No entanto é de facto uma notável oportunidade o RGPD nas entidades públicas, pois vem atualizar os procedimentos, de acordo com a segurança e privacidade, bem como a gestão de dados.

O RGPD torna-se, assim, responsabilidade de cada entidade pública, através da efetivação na implementação, determinando os trâmites essenciais para garantir *compliance* no decorrer da sua atividade. Esta implementação recai na responsabilidade do responsável pelo tratamento, analisado de seguida em maior pormenor (art.º 24, (UE) 2016/679).

Uma proposta de plano de ação, dividido em cinco fases, é apresentada pela Presidência do Conselho de Ministros:

Figura 10: Proposta de plano de ação para implementação RGPD



Fonte: Presidência do Conselho de Ministros, 2021.

Enquanto Francisco e Francisco estruturam um trabalho de execução em 7 passos:

> Planear bem o trabalho, mapear todos os dados pessoais tratados na organização, caracterizar os tratamentos tal como são realizados à data, identificar as atividades que carecem de alteração e quais as que têm maior risco, implementar as alterações, verificar a conformidade e garantir a compatibilidade tecnológica, constituir um dossier com as evidências de implementação, avaliar o impacto do projeto, formar os colaboradores da organização e criar as condições para que a organização integre, no seu funcionamento, estruturas e cultura organizacional, a monitorização e a conformidade com o RGPD, (2019, p. 60).

Conforme já descrito a implementação do RGPD requer que a organização possua um *know-how* abrangente de todos os seus procedimentos de tratamento de dados pessoais, o que significa fazer um levantamento dos mesmos, através do seu registo (no art.º 30, (UE) 2016/679). Resumidamente, importa quanto ao tratamento determinar: as finalidades, as bases de licitude, as categorias e datas-limite de preservação dos mesmos e por outro lado, determinar as categorias de titulares e destinatários de dados pessoais. Bem como, delinear medidas técnicas e organizativas. Para esta concretização a CNPD dispõe um *template* de registo de atividades de tratamento, no seu endereço *web*:

Quadro 10: *Template* de registo de atividades de tratamento.

Tratamento	**Finalidade**	**Categoria dos dados tratados**	**Dados e prazo de conservação**	
			Dados de identificação	ex: nome, fotografia, número de identificação civil ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual
			Dados de contacto	ex: morada, e-mail, telefone
			Dados de faturação	ex: NIF, montante cobrado, data, IBAN
			Vida familiar	ex: situação familiar, dados do agregado familiar, estado civil
			Vida profissional	ex: CV, situação profissional, escolaridade, formação, distinções, diplomas
			Informações de ordem financeira e patrimonial	ex: vencimento, situação financeira, dados bancários, rendimentos, património
			Dados de tráfego e de localização	ex: endereços IP, *logs*, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos *wi-fi*
			Dados de navegação na internet	ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, *device fingerprinting*, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização
			Outras categorias de dados pessoais não sensíveis	ex: cor dos sapatos na festa de Natal

			Perfis	ex: hábitos de vida, bom devedor, saudável
			Art.º 9.º, n.º 1 - Regulamento (UE) 2016/679	Sim/Não ex: sim > origem racial ou étnica, opiniões políticas, convicções religiosas e filosóficas, filiação sindical, dados genéticos, dados biométricos (controlo de acesso físico, controlo de acesso lógico), dados sobre a saúde, a vida sexual e a orientação sexual
			Art.º 10.º - Regulamento (UE) 2016/679	Sim/Não ex: sim > dados relativos às condenações e às infrações penais
			Categorias titulares dados: RH; Clientes; Potenciais clientes; Fornec.	Sim/Não
			Fundamento de Licitude	ex: Consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúde, interesse público ou exercício de autoridade pública

Fonte: Adaptado do modelo de registo para subcontratantes da CNPD (2021).

Ao delinear todos estes elementos do tratamento, também é importante que este método se aplique a processos e políticas, assegurando e demonstrando conformidade face às especificações obrigatórias do RGPD. Principalmente através da criação e divulgação de políticas de privacidade e de proteção de dados, garantindo acesso, informação e prazos (por exemplo) a todos os titulares de dados pessoais. E por fim o contato do EPD.

Deste modo, é aconselhado que a organização desenvolva as suas próprias políticas internas e formulários "para o exercício de direitos, assim como uma política de resposta às solicitações do titular dos dados e de resposta a violações de dados pessoais, elaborando minutas de notificação." (Teves, 2019, p. 106). A mesma autora indica a criação de um "procedimento para a avaliação do impacto de proteção de dados (ex. aplicação da norma ISO 31000:2009)", bem como, que sejam analisados os "sistemas de tecnologia da informação e adotadas medidas de segurança no tratamento" (Teves, 2019, p. 106).

Aliado a toda esta questão é também importante o facto de as entidades públicas estarem sujeitas ao Código dos Contratos Públicos (CCP) no momento de contratação (art.º 2, nº 1, Decreto-Lei n.º 18/2008, de 29 de janeiro), pelo que se torna imperioso que estes contratos também estejam em conformidade, com o RGPD.

Neste caso Teves (2019) aconselha uma cláusula de proteção de dados, que encarregue o subcontratante por respeitar estas obrigações e que controle os trâmites do tratamento a efetuar. Para que os contratos já vigentes também disfrutem desta nova tramitação normativa, é importante que sejam analisadas e definidas as modificações necessárias.

O sistema de gestão e de segurança da informação tem que ser revisto pela AP, prevenindo acessos ou até divulgações de informações não autorizadas. É obrigatório que as entidades públicas designem um *Data Protection Officer* (DPO) ou EPD, para ter como sua principal função o auxílio na implementação de renovadas regras (Vitorino, 2018).

Entendem-se por entidades públicas, segundo o art.º 12, nº 2, da Lei n.º 58/2019:

1. O Estado;
2. As regiões autónomas;
3. As autarquias locais e as entidades supranacionais previstas na lei;
4. As entidades administrativas independentes e o Banco de Portugal;
5. Os institutos públicos;
6. As instituições de ensino superior públicas, independentemente da sua natureza;
7. As empresas do setor empresarial do Estado e dos setores empresariais regionais e locais;
8. As associações públicas.

O RGPD também define que as entidades públicas devem nomear um EPD, sempre que o: "tratamento for efetuado por (…) um organismo público" e quando o "controlo regular e sistemático dos titulares dos dados em grande escala" encontra-se em causa, (art.º 37, nº1, a) e b), (UE) 2016/679).

Face a esta nova exigência, Lambert (2017) salienta a criação de uma nova profissão, face ao regime de proteção de dados e as suas questões. De forma sucinta e resumida, apresentam-se as medidas a serem implementadas, segundo Vitorino (2018):

1. Designar o DPO;
2. Criar um grupo de trabalho multidisciplinar;
3. Realizar um diagnóstico e levantamento das operações de tratamento;
4. Rever a licitude do tratamento;
5. Rever políticas e procedimentos internos, contratos;
6. Implementar um registo das atividades de tratamento;
7. Avaliar e rever a adequação dos sistemas de gestão e de segurança da informação.

Figura 11: EPD nas entidades públicas

"Independentemente de quem seja responsável pelo tratamento, **existe pelo menos um encarregado de proteção de dados**:
a) Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respetivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;
b) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respetivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;
c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;
d) Nas freguesias em que tal se justifique, nomeadamente naquelas com mais de 750 habitantes, sendo designado pela junta de freguesia, com faculdade de delegação no presidente;
e) Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação no respetivo presidente".

Fonte: art.º 12, nº 3, Lei n.º 58/2019.

De acordo com a Comissão Europeia (2020), as administrações públicas "têm a obrigação de nomear um encarregado da proteção de dados (EPD), embora seja possível nomear um único encarregado da proteção de dados para vários organismos públicos, que poderão assim partilhar os seus serviços ou subcontratar esta tarefa a um EPD externo".

Figura 12: Funções do encarregado da proteção de dados

Funções do encarregado da proteção de dados:

- "O encarregado da proteção de dados tem, pelo menos, as seguintes funções:
- a) **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;
- 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 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;
- 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 do artigo 35.º;
- 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, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto".

Fonte: art.º 39, nº1, (UE) 2016/679.

A função do EPD não poderá emergir num conflito de interesses (art.º 38, nº6, (UE) 2016/679), ou seja, deve desempenhar as suas funções com autonomia e independência. Mais especificamente o EPD é quem tem a habilitação para certificar se o RGPD está a ser minuciosamente executado pelo responsável (ou subcontratante) no tratamento de dados pessoais. Este poderá ainda recomendar e sugerir determinações no tratamento, bem como, recolher informações sobre as operações do responsável (ou subcontratante).

O EPD deverá estar em contato com todas as fases de proteção de dados, em tempo útil (art.º 38, nº1, (UE) 2016/679), facto garantido pelo responsável. Embora o responsável, em momento algum pode dar orientações sobre como desenvolver as suas funções ou auxiliar na tomada de decisões. Como reforço da sua autonomia, o EPD não pode ser penalizado por desenvolver as suas funções (art.º 38, nº3, (UE) 2016/679).

Sendo assim, o EPD, o responsável e o subcontratante no que respeita ao tratamento de dados, todos têm de cumprir o disposto no RGPD, contudo, o primeiro apenas coopera com a organização e a autoridade de controlo (conforme na figura anterior), no controlo sistemático do tratamento de dados pessoais.

O indivíduo selecionado terá de apresentar conhecimentos específicos no que concerne às práticas de proteção de dados, colaborando com a implementação das práticas de RGPD. Deste modo, é bastante palpável a necessidade de uma pessoa para o cargo, com capacidades para o mesmo, pois como declaram autores como Vitorino (2018), as entidades públicas ficam sujeitas a coimas e quando ocorre uma violação dos dados pessoais pela AP, o cidadão pode requerer uma indemnização.

Como qualidades do EPD, segundo Teles (2020), destacam-se:

- Competências no domínio das legislações e práticas nacionais e europeia
- Conhecimento das operações de tratamento efetuadas, bem como, dos sistemas de informação, da segurança e das necessidades de proteção de dados
- Conhecimento profundo do RGPD
- Formação em Proteção de Dados

Os requisitos a nível profissional não devem ser os únicos, também são importantes as aptidões pessoais, como a integridade e ética segundo Cunha *et al.* (2020). Estes autores vão mais longe e defendem a enorme versatilidade, aptidão de pensar "fora da caixa", bem como, um pouco de criatividade do desenvolver da atividade. Neste sentido, Butarelli (2018) destaca: "*Today, ethics and data protection are intertwined like never before and I observe an ever closer convergence between the two*" (2018, p. 1).

Não obstante o EPD está impelido ao dever de sigilo e confidencialidade relativamente a tudo em relação às suas funções (art.º 10, Lei 58/2019 e art.º 38, nº5, (UE) 2016/679).

Por fim, Oliveira *et al.* (2020) salientam que a Gestão Documental (GD), vem a ser bastante útil para esta perspetiva e inserção do regulamento pois, assim, irá gerir um ciclo de vida dos dados pessoais mais organizado. É importante também evidenciar que "é a partir da gestão documental que podemos ajudar a trazer respostas para a instituição que pretende gerir bem seus dados pessoais, inevitavelmente presente em documentos e informações" (Pessoa, 2020, p. 258). Bem como, é necessária uma boa logística no âmbito da GD, devido à extensão de dados e tratamentos.

Numa perspetiva de incumprimento de algumas determinações legais face ao abordado até aqui, podem ocorrer comprometimentos criminais, civis ou contraordenações nacionais. Nesta situação a CNPD pode ainda aplicar sanções acessórias, se assim o entender. Neste caso, é o responsável (ou subcontratante) pelo tratamento que aufere a responsabilidade do cumprimento do regulamento, pois "aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade" (art.º 24, nº1, (UE) 2016/679). Uma outra questão a ter em conta é o facto da imagem e reputação das organizações poderem sempre ser postas em causa, havendo aqui uma conotação bastante negativa. Embora já se incorra em crime quando:

Quadro 11: Lista das contraordenações e punições face ao tratamento de dados

Contraordenação	Lei n.º 58/2019 > Punição
Utilização de dados de forma incompatível com a finalidade da recolha Utilização ou manuseamento de **dados pessoais de modo incompatível com a finalidade da recolha**	"**pena de prisão até um ano ou com pena de multa até 120 dias**." E a "pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD." (art.º 46, Lei n.º 58/2019).
Acesso indevido Utilização ou manuseamento **sem a autorização ou justificação obrigatória**, **aceder**, por qualquer modo a **dados pessoais**.	"**pena de prisão até 1 ano ou com pena de multa até 120 dias**." Esta é "agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD. 3 — A pena é também agravada para o dobro nos seus limites quando o acesso: a) For conseguido através de violação de regras técnicas de segurança; ou b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial." (art.º 47, Lei n.º 58/2019).

Desvio de dados Utilização ou manuseamento que implica **copiar, subtrair, ceder ou transferir,** a título oneroso ou gratuito, dados pessoais **sem previsão legal ou consentimento,** apesar da finalidade.	"prisão até 1 ano ou com pena de multa até 120 dias." E a "pena é agravada para o dobro nos seus limites quando se tratar dos dados pessoais a que se referem os artigos 9.º e 10.º do RGPD. 3 — A pena é também agravada para o dobro nos seus limites quando o acesso: a) For conseguido através de violação de regras técnicas de segurança; ou b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial." (art.º 48, Lei n.º 58/2019).
Viciação ou destruição de dados Utilização ou manuseamento que implica **apagar, destruir, danificar, ocultar, suprimir ou modificar** dados pessoais, **sem** a devida **autorização ou justificação**, tornando-os **inutilizáveis ou afetando o seu potencial de utilização.**	"pena de prisão até 2 anos ou com pena de multa até 240 dias. E a "pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave. 3 — Nas situações previstas nos números anteriores, se o agente atuar com negligência é punido com pena de prisão: a) Até 1 ano ou multa até 120 dias, no caso previsto no n.º 1; b) Até 2 anos ou multa até 240 dias, no caso previsto no n.º 2." (art.º 49, Lei n.º 58/2019).
Inserção de dados falsos Utilização ou manuseamento que implica **inserir ou facilitar a inserção de dados pessoais falsos**, com a **intenção de obter vantagem indevida** para si ou para terceiro, **ou** para **causar prejuízo.**	**"**pena de prisão até 2 anos ou com pena de multa até 240 dias." E a "pena é agravada para o dobro nos seus limites se da inserção referida no número anterior resultar um prejuízo efetivo." (art.º 50, Lei n.º 58/2019).
Violação do dever de sigilo Utilização ou manuseamento que implica Quem, **sem justa causa** e devido **consentimento**, **revelar ou divulgar** no todo ou em parte dados pessoais, estando **obrigado a sigilo profissional** nos termos da lei.	"pena de prisão até 1 ano ou com pena de multa até 120 dias." E a "pena é agravada para o dobro nos seus limites se o agente: a) For trabalhador em funções públicas ou equiparado, nos termos da lei penal; b) For encarregado de proteção de dados; c) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo; d) Puser em perigo a reputação, a honra ou a intimidade da vida privada de terceiros. 3 — A negligência é punível com pena de prisão até 6 meses ou com pena de multa até 60 dias." (art.º 51, Lei n.º 58/2019).
Desobediência Quem **ultrapassar os prazos afixados pela CNPD**, para **cumprir obrigações** previstas no **RGPD** e na presente lei.	"pena de prisão até 1 ano ou com pena de multa até 120 dias." E a "pena é agravada para o dobro nos seus limites se, depois de notificado para o efeito, o agente: a) Não interromper, cessar ou bloquear o tratamento ilícito de dados; b) Não proceder ao apagamento ou destruição dos dados quando legalmente exigível, ou findo o prazo de conservação fixado nos termos da presente lei; ou c)

	Recusar, sem justa causa, a colaboração que lhe for exigida nos termos do artigo 8.º da presente lei." (art.º 52, Lei n.º 58/2019).
Punibilidade da tentativa	"Nos crimes previstos na presente secção, a tentativa é sempre punível" (art.º 53, Lei n.º 58/2019).
Responsabilidade das pessoas coletivas Pessoas coletivas e entidades equiparadas, com exceção do Estado.	"no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos na presente secção, nos termos do artigo 11.º do Código Penal." (art.º 54, Lei n.º 58/2019).

Fonte: Elaboração própria, segundo a Lei n.º 58/2019.

As contraordenações muito graves estão identificadas e estipuladas no art.º 37 da Lei 58/2019, já as graves estão no artigo seguinte.

Face ao exposto sentimos necessidade de explorar as avaliações de impacto sobre a proteção de dados (AIPD). Este trata-se de um processo projetado para acompanhar o tratamento de dados pessoais por forma a "avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos" face os direitos e liberdades dos titulares (GT29, 2017, p4). O objetivo desta avaliação é deliberar as medidas indispensáveis para responder a esses riscos. Uma grande vantagem destas avaliações é a responsabilização, já que permite auxiliar os responsáveis no tratamento, a cumprir os requisitos do RGPD, mas também expor que as medidas adequadas para assegurar a conformidade, com o regulamento foram executadas.

"Uma AIPD é um processo que visa estabelecer e demonstrar conformidade" (GT29, 2017, p4)., por isso, quando é que se torna imperativo realizar uma AIPD? E o que deve incluir? Segundo o art.º 35, nº3, (UE) 2016/679, a AIPD é obrigatória quando:

- a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
- b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou
- c) Controlo sistemático de zonas acessíveis ao público em grande escala.

O responsável pelo tratamento de dados também se deverá encarregar da realização de uma AIPD, quando estão em causa operações de tratamento vulneráveis a elevado risco para os direitos e liberdades das pessoas singulares (Considerações 84) e 90), (UE) 2016/679.). A AIPD deve incluir:

a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

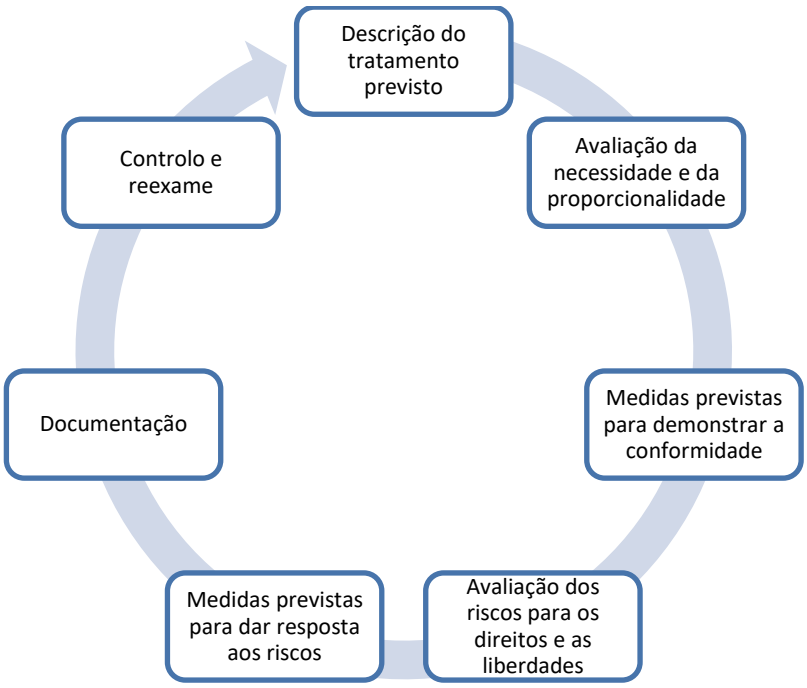
b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa (art.º 35, nº7, (UE) 2016/679).

Face ao exposto, é obrigação do responsável pelo tratamento estruturar e delinear um guia que faculte os trâmites a desenvolver no tratamento de dados pessoais. Neste contexto, o GT29 apresenta a metodologia do processo iterativo genérico, para a realização de uma AIPD (figura 13).

Figura 13: Processo iterativo genérico para a realização de uma AIPD



Fonte: Adaptação do GT29, 2017, p. 19.

Esta prática numa organização é sinónimo de atuar em conformidade com o regulamento. Conquistando uma planificação conforme, que garanta um nível máximo de segurança, no tratamento de dados pessoais. As regras convencionadas numa AIPD precisam ser obedecidas, por forma a que transmitam numa "maior confiança por parte dos titulares dos dados para com os responsáveis pelo tratamento de dados" (GT29, 2017, p. 23).

3.2 O ACESSO A DOCUMENTOS ADMINISTRATIVOS E A PROTEÇÃO DE DADOS

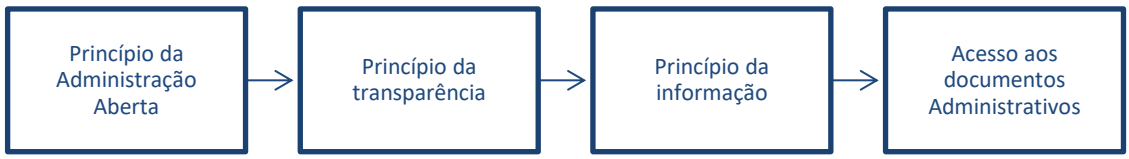
Este novo enquadramento de proteção de dados na AP obriga à simultaneidade de articulação com o regime de acesso aos documentos administrativos. Por um lado, temos o direito à liberdade de expressão e de informação (art.º 11, CDFUE e o art.º 10, Convenção Europeia dos Direitos Humanos), que consiste no poder de transmitir e receber informações (sem intromissões públicas ou fronteiras). E por outro, temos o direito de acesso a documentos oficiais sem barreiras (art.º 15, nº3, Tratado sobre o Funcionamento da União Europeia (TSFUE)), que constitui o poder de ter acesso a documentos das instituições, órgãos e organismos da União, sujeitos a princípios, condições e limites (Regulamento (CE) n.º 1049/2001).

Esta faculdade de receber informações garante transparência das operações administrativas numa comunidade democrática, assegurando uma participação mais forte do cidadão, nos procedimentos de deliberação. Por outro lado, a garantia de acesso mais amplo e facilitado aos documentos é regida por princípios, condições e limites que salvaguardam os interesses públicos e privados, promovendo práticas administrativas positivas (art.º 15, TSFUE).

Em termos nacionais a CRP determina que o acesso a dados pessoais de terceiros é proibido (art.º 35, nº4, CRP), já o RGPD pressupõe que o tratamento de dados pessoais (acesso), seja legítimo (art.º 6, (UE) 2016/679).

Já face à disposição jurídica portuguesa, o acesso aos documentos administrativos e à informação administrativa, integra o rol constitucional dos direitos e garantias dos administrados, ao garantir o acesso a dados pessoais de terceiros, nos casos que se confirmem as condições da Lei n.º 26/2016. Apresentamos de seguida os princípios orientadores do acesso aos documentos administrativos:

Figura 14: Princípios orientadores do acesso aos documentos administrativos



Fonte: Elaboração própria, segundo o art.º 2 da Lei n.º 26/2016.

Ao analisarmos o Princípio da Administração Aberta (PAA), conseguimos perceber que para este garantir o acesso livre e universal aos dados administrativos é necessário a transparência da atividade administrativa, a divulgação e a disponibilização de informação (art.º 2, Lei n.º 26/2016, de 22 de agosto). Sendo assim, a AP encontra-se vinculada pelos princípios guias da operacionalização administrativa, que credenciam a sua própria autonomia de atuação.

Figura 15: Direitos e garantias dos administrados

Direitos e garantias dos administrados:

- 1. Os cidadãos têm o direito de ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam diretamente interessados, bem como o de conhecer as resoluções definitivas que sobre eles forem tomadas.
- 2. Os cidadãos têm também o **direito de acesso aos arquivos e registos administrativos**, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas.
- 3. Os atos administrativos estão sujeitos a notificação aos interessados, na forma prevista na lei, e carecem de fundamentação expressa e acessível quando afetem direitos ou interesses legalmente protegidos.
- 4. É garantido aos administrados tutela jurisdicional efetiva dos seus direitos ou interesses legalmente protegidos, incluindo, nomeadamente, o reconhecimento desses direitos ou interesses, a impugnação de quaisquer atos administrativos que os lesem, independentemente da sua forma, a determinação da prática de atos administrativos legalmente devidos e a adoção de medidas cautelares adequadas.
- 5. Os cidadãos têm igualmente direito de impugnar as normas administrativas com eficácia externa lesivas dos seus direitos ou interesses legalmente protegidos.
- 6. Para efeitos dos n.os 1 e 2, a lei fixará um prazo máximo de resposta por parte da Administração.

Fonte: art.º 268, CRP.

Conforme se pode constatar o PAA está disposto no nº 2, do artigo transcrito (art.º 268, CRP), embora a CRP também contempla o direito à informação (art.º 37, CRP) e o direito à participação na vida pública (art.º 48, CRP).

Já no caso do Código do Procedimento Administrativo (CPA – Decreto-Lei n.º 4/2015, de 07 de Janeiro) estão consagrados para todas as pessoas, o direito "à proteção dos seus dados pessoais e à

segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito" (art.º 18, CPA) e o "direito de acesso aos arquivos e registos administrativos, mesmo quando nenhum procedimento que lhes diga diretamente respeito esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas" (art.º 17, CPA).

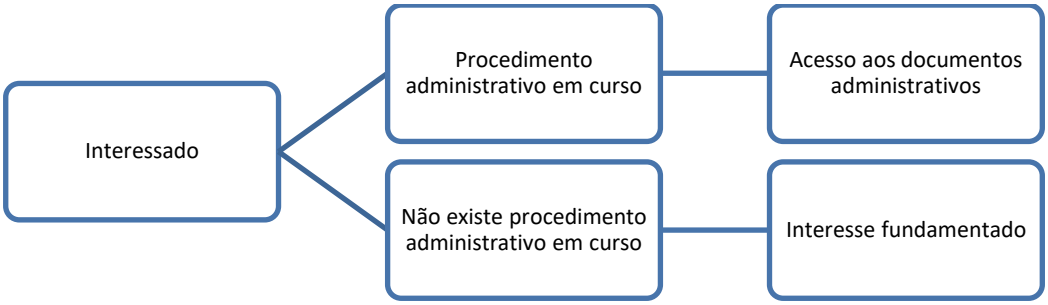
O PAA encontra-se também previsto no artigo 2, da Lei 26/2016 de 22 de agosto, que contempla o processo de permissão à informação administrativa e ambiental e de reutilização dos documentos administrativos (transpondo a Diretiva 2003/4/CE), mas salvaguardando "princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares" (art.º 2, nº1, Lei 26/2016). Considera-se ainda, essencial a prevalência da transparência da atividade administrativa, bem como, o direito à informação dos cidadãos (art.º 2, nº2 e nº3, Lei 26/2016).

Apesar da CRP não normalizar o princípio da transparência como princípio fundamental na AP, existem normas sobre esta matéria como acabamos de ver. Todavia, Fernandes (2015, p. 436) esclarece que este princípio "impõe a visibilidade e proíbe a opacidade do funcionamento e da atuação da Administração", ou seja, este "princípio da transparência obriga a que a organização e o procedimento administrativos estejam regulados e ordenados, por um lado, e que a Administração sempre se comporte, por outro, de tal modo que seja permitido ver para dentro da Administração".

Quanto ao direito à informação este encontra-se estipulado na CRP (art.º 37) e o princípio da colaboração com os particulares está disposto no CPA (art.º 11) e encontra-se também afeto à AP. Sendo assim, a AP deve operacionalizar em colaboração com os particulares, prestando-lhes informações e esclarecimentos. A AP deve também reger-se pelo princípio da participação (art.º 12, CPA), que garante a participação dos procedimentos na geração das decisões que lhes digam respeito e o direito dos interessados à informação (art.º 82, CPA), que garante que os interessados são informados sobre o estado dos procedimentos a seu respeito, bem como o direito de saber as resoluções definitivas que sobre eles forem executadas. Embora este último abranja qualquer pessoa que prove legitimidade no conhecimento dos elementos que pretende (art.º 85, CPA).

De seguida apresenta-se o esquema de como se processa o acesso a um documento administrativo na AP.

Figura 16: Acesso a documentos administrativos



Fonte: Adaptado de Teves (2019).

Uma operacionalização administrativa em curso tem de garantir cumulativamente, o direito à informação, o direito ao acesso a documentos administrativos e o princípio da colaboração com os particulares, no decurso de um procedimento administrativo.

No caso de não subsistir um procedimento administrativo em curso para o cidadão, mas apresente um interesse fundamentado neste procedimento, subsiste o nº 2, do artigo 268, da CRP.

O direito ao acesso a documentos administrativos não estabelece um direito absoluto e ilimitado, ou seja, este pode sofrer limitações quanto à reserva da intimidade da vida privada, por exemplo. Embora ao ponderar a amplitude das normas constitucionais dos direitos, liberdades e garantias ao direito de acesso a documentos administrativos (art.º 17 e 18, CRP), existem restrições admissíveis que têm de ser constitucionalmente permitidas, determinadas por lei, contidas nos limites do princípio da proporcionalidade e ser empregues nos seus parâmetros (Provedor de Justiça, 2006).

Um destes exemplos deriva da reserva da intimidade da vida privada e familiar, que assegura a todos os indivíduos este direito, transpondo-se na não autorização de acesso e divulgação de dados pessoais de terceiros. Logo, em caso de conflito entre o direito de acesso e o direito à reserva da intimidade da vida privada prevalece a finalidade,

> sendo que só são legitimados sacrifícios do direito fundamental do direito de acesso aos arquivos e registos administrativos perante direitos e valores constitucionais de igual ou superior valor, designadamente, relativos à segurança interna e externa, à investigação criminal e à reserva da intimidade da vida privada (Teves, 2019, p. 124).

Nesta dicotomia com o objetivo de eliminar estes casos de violação dos dados pessoais, torna-se assim premente o conceito de interessado e a sua latência. Entra assim em primeiro plano o CPA

que define que os "particulares têm o direito de intervir pessoalmente no procedimento administrativo ou de nele se fazer representar ou assistir através de mandatário" (art.º 67, nº1, CPA).

Os titulares possuem ainda a "legitimidade para iniciar o procedimento ou para nele se constituírem como interessados os titulares de direitos, interesses legalmente protegidos, deveres, encargos, ónus ou sujeições no âmbito das decisões que nele forem ou possam ser tomadas", também estão afetas as "associações, para defender interesses coletivos ou proceder à defesa coletiva de interesses individuais dos seus associados que caibam no âmbito dos respetivos fins" (art.º 68, nº1, CPA).

Posto isto, acautelando a salvaguarda da proteção dos dados pessoais, também não se deverá limitar à demonstração de interesse legitimo, importa garantir sempre o princípio da transparência e o direito a acesso a documentos administrativos, em contraponto com as finalidades de tratamento e os fundamentos de licitude de tratamento de dados pessoais.

Neste contexto, importa também definir o que é um documento administrativo e um documento nominativo, direito de acesso e restrições em ambos os casos.

Quadro 12: Definição Documento Administrativo, contemplação do Direito de Acesso e Restrições

Lei n.º 26/2016, de 22 de agosto	
Definição documento administrativo	"**qualquer conteúdo**, ou parte desse conteúdo, que esteja na **posse** ou seja detida em nome dos **órgãos e entidades** referidas no artigo seguinte, seja o suporte de informação sob **forma** escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a: i) Procedimentos de emissão de atos e regulamentos administrativos; ii) Procedimentos de contratação pública, incluindo os contratos celebrados; iii) Gestão orçamental e financeira dos órgãos e entidades; iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas" (art.º 3, nº 1, a), Lei n.º 26/2016).
Direito de acesso	"Todos, sem necessidade de enunciar qualquer interesse, têm **direito de acesso aos documentos administrativos**, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo." e "O direito de acesso realiza-se independentemente da integração dos documentos administrativos em arquivo corrente, intermédio ou definitivo." (art.º 5, nº 1 e 2, Lei n.º 26/2016).
Restrições ao direito de acesso	"Os documentos que contenham **informações cujo conhecimento seja avaliado como podendo pôr em risco interesses fundamentais do Estado** ficam sujeitos a interdição de acesso ou a acesso sob autorização, durante o tempo estritamente necessário (…) Os documentos **protegidos por direitos de autor ou direitos conexos** (…) O acesso aos documentos administrativos preparatórios de uma

	decisão ou constantes de **processos não concluídos** pode ser diferido até à tomada de decisão, ao arquivamento do processo ou ao decurso (…) O acesso ao conteúdo de **auditorias, inspeções, inquéritos, sindicâncias ou averiguações** pode ser diferido até ao decurso do prazo para instauração de procedimento disciplinar." (art.º 6, nº 1 ao 4, Lei n.º 26/2016).

Fonte: Elaboração própria, segundo Lei n.º 26/2016.

Quadro 13: Definição Documento Nominativo e Restrições de acesso

Lei n.º 26/2016, de 22 de agosto	
Definição documento nominativo	"o documento que **contenha dados pessoais**, na **aceção do regime jurídico de proteção das pessoas singulares** no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (art.º 3, nº 1, b), Lei n.º 26/2016).
Restrições ao direito de acesso	"Um **terceiro só tem direito de acesso** a documentos nominativos: a) Se estiver **munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade** e quanto ao **tipo** de dados a que quer aceder; b) Se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação." (art.º 6, nº 5, Lei n.º 26/2016). "Os documentos nominativos **comunicados a terceiros não podem ser utilizados ou reproduzidos de forma incompatível com a autorização concedida**, com o fundamento do acesso, com a finalidade determinante da recolha ou com o instrumento de legalização, sob pena de responsabilidade por perdas e danos e responsabilidade criminal, nos termos legais." (art.º 8, nº 2, Lei n.º 26/2016).

Fonte: Elaboração própria, segundo Lei n.º 26/2016.

Enquanto o documento administrativo pode ganhar diferentes formas e âmbitos de qualquer conteúdo, o documento nominativo, já só se refere explicitamente a conteúdos, com dados pessoais.

Quando um documento administrativo se encontra restrito no seu acesso, deve ser objeto de uma comunicação parcial, assim que se demonstre possível a expurgação da informação sobre a matéria reservada (art.º 6, nº 8, Lei n.º 26/2016). Sendo assim, mesmo existindo um interesse legítimo por parte de terceiros, sobrepõe-se um acesso limitado e não um acesso ilimitado.

Contrapõe-se assim, o conceito de interesse legítimo como algo impreciso, uma vez que coloca em causa interesses particulares vários (económicos, por exemplo), pelo que cabe à entidade pública determinar os conflitos de interesse. É importante avaliar o proveito que o particular requer, os princípios e garantidas que têm de ser instituídos por estas entidades, face aos dados particulares em causa que têm de salvaguardar e ainda fundamentar a sua decisão, segundo a proporcionalidade e razoabilidade.

Como resposta a esta questão arbitrária do interesse legítimo temos a Comissão de Acesso a Documentos Administrativos (CADA) e a CNPD, que se encontram aptas para se articular sobre o acesso a dados pessoais. Embora, para que seja claro o regime legal aplicável neste contexto, também há que colocar em perspetiva a Lei n.º 26/2016 e o RGPD.

A CADA trata-se de uma entidade administrativa autónoma junto da Assembleia da República (art.º 28, nº 1, Lei n.º 26/2016), que tem o objetivo de garantir o cumprimento da Lei n.º 26/2016, sendo da sua responsabilidade apreciar queixas ou emitir pareceres, sobre o acesso a documentos administrativos (art.º 30, Lei n.º 26/2016).

Andrade (2004, cit. por Gouveia, 2015) alerta: "Na metodologia para resolução de conflitos entre direitos, tem de atender-se fundamentalmente a três factores, ponderando, num juízo global, mas em função de cada um deles, todas as circunstâncias relevantes no caso concreto", depois referindo o "âmbito e graduação do conteúdo dos preceitos constitucionais em conflito (…), a natureza do caso (…) e a condição e o comportamento das pessoas envolvidas (…)" (pp. 77-78).

Resumindo, quando está em causa o acesso a informação administrativa com requisitos nominativos, o enfoque tem de ser dado à finalidade de tratamento de dados pessoais, sendo responsabilidade da entidade pública determinar o veto ou aceitação do acesso, face aos critérios de proporcionalidade. Neste caso, para a entidade determinar se temos dados que necessitam de proteção é importante analisar: o direito à privacidade do titular e a informação limitar-se ao estritamente necessário, face à finalidade invocada (comunicação parcial quando possível).

Sempre que se verifique uma situação de conflito entre o direito de acesso e o direito à reserva da intimidade da vida privada, prevalece a finalidade, embora só se torna legitimo o sacrifício do direito fundamental, do direito de acesso aos documentos administrativos (repositórios e registos), quando estão em causa direitos e valores constitucionais de igual ou superior valor, como por exemplo, relativos à segurança interna e externa e à investigação criminal.

3.3 GESTÃO DOCUMENTAL

O mundo digital veio exigir que as organizações optassem por diferentes medidas práticas face ao seu contexto, em contraponto de uma realidade limitada à dimensão física dos acervos. Em que impera a acomodação de funcionalidades como: "produção, fluxo, armazenamento, gestão, transmissão e uso/reprodução de informação em todo o seu ciclo de vida", independentemente do estado físico ou espacial (Pinto, 2013, p. 10).

A Sociedade da Informação (SI) é igualmente uma realidade que se estabelece, derivada deste novo contexto e que adota três características essenciais: uso intensivo das TIC, uso crescente do digital e a organização em rede (Gouveia, 2017). E, por conseguinte, a informação (interna e externa) gerada e disponibilizada aos gestores vai permitir maior segregação, posterior valorização do fluxo de informação e auxiliar a tomada de decisões (Lei da sobrevivência de Murdick).

Mas, para que esta realidade seja conseguida, existe a necessidade de convergência da documentação de suporte analógico para digital, ou seja a desmaterialização da informação (António, 2009). Sendo assim, o meio digital impõe duas grandes razões para a adoção de sistemas de *software* na GD: a sustentabilidade destes sistemas (papel e a sua degradação) e a diversidade de documentos eletrónicos que dependem de práticas eletrónicas de gestão de conteúdos, com o intuito de acesso futuro (Nguyen, Swatman & Fraunholz, 2007). A gestão de documentos eletrónicos compreende como principais etapas:

- "Criação de documentos ("analógicos" e nadodigitais);
- Captura ou digitalização;
- Gestão de imagens, documentos e registos (meta-informação associada);
- Partilha ou divulgação; Segurança;
- Automação dos fluxos de trabalho (*workflows*);
- Armazenamento;
- Preservação;
- Incorporação com outros sistemas dentro da organização" (Pinto, 2018, p. 27).

Gestão da Informação, segundo o *Harrod´s Librarians´ Glossary,* é "un imprecise term for the various activities" orientadas para a geração, coordenação, armazenamento ou conservação, busca e recuperação da informação, tanto interna como externa, contida em qualquer suporte" (Prytherch, 2005, cit. por Gomes, 2016, p. 131).

Gomes (2016, p. 132), por um lado ressalva a ideia trazida por Choo (2003), que defende que "a GI compreende um conjunto de atividades encadeadas e relacionadas com todo o ciclo

informacional, em suportes analógicos e/ou digitais", por outro lado refere, segundo Prytherch (2005), que a Gestão da Informação abrange todo o ciclo informacional.

Relativamente à GD, esta é definida como um conjunto de procedimentos que consistem em: criar, organizar, utilizar, conservar, avaliar, selecionar e eliminar documentos. Desenvolve-se num "campo da gestão responsável por um controlo eficiente e sistemático da produção, recepção, manutenção, utilização e destino dos documentos de arquivo, incluindo os processos para constituir e manter prova e informação sobre actividades e transacções a gestão documental" (Instituto dos Arquivos Nacionais / Torre de Tombo, 2006, p. 5). Esta linha de pensamento assume o ciclo de vida continuado do documento (*records continuum*) como objeto, independentemente o período de vida em que se encontra, subsistindo as várias solicitações dos utilizadores, às quais correspondem procedimentos específicos de gestão (Instituto dos Arquivos Nacionais / Torre de Tombo, 2016).

A GD tem como objetivo controlar a criação, o armazenamento e a avaliação/seleção dos "records", uma vez que estes são entendidos como documentos produzidos e recebidos por uma organização (pública ou privada), no desenvolvimento da sua atividade e por ela preservados, como prova dos seus procedimentos e transações (Pinto, 2013).

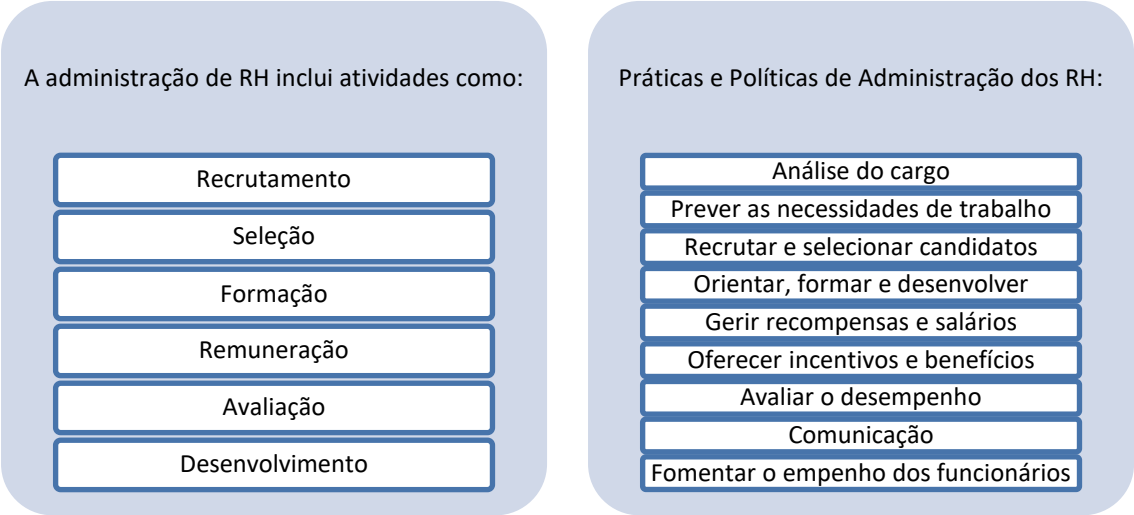
Posto isto, torna-se imperativo que na GD as organizações desenvolvam a implementação de políticas, estratégias e métodos que apoiem transversalmente tarefas como: meios de autenticação eletrónica; gestão de procedimentos e de instrumentos de *workflow*; gestão de *emails*, de conteúdos, de arquivo e de risco, entre outros (Pinto, 2013). Resumidamente, a GD pode adotar duas perspetivas: a arquivística (impacto da SI) e a informática (progresso tecnológico na SI).

Sempre que são mencionadas a gestão documental ou a gestão de documentos, significa que estamos a aludir à gestão de informação (ou arquivística). O sistema de informação é a integração de um conjunto de componentes que visam auxiliar a operacionalidade da organização (Lares & Karen, 2005). Neste caso, a implementação do sistema de informação tecnológico centra-se na sua aplicação prática e não apenas no emprego de *hardware.*

Em contexto internacional, a GD foi regida pelas diretrizes editadas em 1979, através do *Records and Archives Management Programme* (RAMP). Posteriormente, surge a ISO 15489:2001 que aborda as generalidades (parte 1) e as diretrizes (parte 2) da gestão de documentos. Por fim, temos a norma ISO 26122, em que o foco é a identificação dos procedimentos de trabalho na GD, logo a que causa um impacto maior neste campo.

Um contraponto importante a referir é o facto de existir uma interligação entre a GD e os RH, uma vez que é normalmente esta área/serviço que se responsabiliza pela GD nas organizações, estando aqui incluída toda a informação dos trabalhadores.

Figura 17: Técnicas de administração de RH



Fonte: Elaboração própria, baseada em Dessler (2003).

A GD encontra-se estritamente ligada a outros dois conceitos: *Document Management* e *Records Management*. No caso do *Records Management,* Gestão de Documentos de Arquivo em português, encontra-se regido pela norma NP 4438-1:2005 que o define como "campo da gestão responsável por um controlo eficiente e sistemático da produção, recepção, manutenção, utilização e destino dos documentos de arquivo, incluindo os processos para constituir e manter prova e informação sobre actividades e transacções" (NP 4438-1:2005, cit. por Barros et al., 2008, p. 31).

O documento de arquivo (*records*) é visto como um documento gerado, recebido e conservado, com um objetivo comprovante e informativo por parte de uma organização ou pessoa, no decorrer do desenvolvimento da sua atividade ou dos seus deveres normativos (NP 4438-1:2005, 2005).

Quanto à GD esta subsiste num formato de armazenamento, produção e rastreamento dos documentos e imagens eletrónicas, com o apoio de um *software* adotado por uma organização. Enquanto o documento representa a informação ou objeto submetido, que pode sofrer um tratamento unitário (AIIM, 2021). A GD também pode ser vista como um conjunto de processos que visam gerar, dispor, empregar, preservar, avaliar, selecionar e excluir os documentos, na etapa de arquivo intermédio, bem como, no arquivo definitivo (Instituto dos Arquivos Nacionais / Torre de Tombo, 2016).

Para determinar o sentido da GD é importante que implique:

- Racionalização e automatização de processos de controlo de documentos;

- O aumento da eficiência e da eficácia da organização através de procedimentos de controlo e circulação, armazenamento, eliminação de documentos;
- Racionalização da recuperação da informação documental;
- A garantia de produção e manutenção de fiabilidade, integridade e autenticidade dos documentos capazes de constituir prova das transações a que estes respeitam, (Instituto dos Arquivos Nacionais / Torre do Tombo, 2006, p. 8).

Já quanto ao objetivo, a GD passa pelo domínio da produção, conservação e avaliação de "*records*", sendo estes documentos gerados e recebidos dentro de uma organização (pública ou privada) no decorrer da sua operacionalidade, sendo desta forma preservados, como prova (Webster *et al.*, 1999, cit. por Pinto, 2013). Existindo assim, o enfoque nos procedimentos e estruturas que viabilizam a produção, conservação, recuperação e eliminação da informação, dentro da organização (Webster *et al.*, 1999). Em qualquer entidade a informação é um recurso vital, pelo que o seu tratamento e controlo cada vez em maiores quantidades, sem comprometer a sua qualidade, garante uma vantagem competitiva.

Vê-se ainda como benefícios práticos da implementação da GD, a simplificação do trabalho de arquivo (maior produtividade), a preservação, a conservação e a recuperação célere e explicita de documentos e informação, a eliminação da impossibilidade da adição de documentos e informação (volume), a otimização e libertação dos espaços físicos; o domínio dos procedimentos documentais (entre a conceção, ao último destino) e a simplicidade da partilha ou exclusão dos documentos (Calderon, Cornelsen, Pavezi & Lopes, 2004).

A AP, num contexto de reestruturação e desenvolvimento da GD, deve reger-se pelo conjunto de regulamentos apropriados, os quais não devem ser ignorados. São eles (Lourenço, Penteado & Barros, 2012):

- **Regime geral de arquivos e do património arquivístico** – DL n.º 16/93 em Diário da República: n.º 19, Série I-A, pp. 264-270;
- **Lei orgânica da DGARQ** – DL n.º 93/2007 em Diário da República: nº 63, Série I, pp. 1913-1916;
- **Enquadramento legal da avaliação, seleção e eliminação de documentos** - DL n.º 447/88 em Diário da República: n.º 284, Série I, p. 4885;
- **Substituição de suporte dos documentos** - DL n.º 121/92 em Diário da República: n.º 150, Série I-A, pp. 3146-3147;
- **Regime geral das incorporações** - DL n.º 47/2004 em Diário da República: n.º 53, Série I-A, pp. 1161;
- **Legislação relativa ao papel das Secretarias-gerais na gestão de documentos de arquivo** – Vários os diplomas em contexto do Plano de Redução e Melhoria da Administração Central

(PREMAC) e do Programa de Reestruturação da Administração Central do Estado (PRACE) que se encontram em vigor;

- **Acesso aos documentos dos organismos públicos e proteção dos dados pessoais** –Lei n.º 67/98 em Diário da República: n.º 247, Série I-A, pp. 5536-5546 e a Lei n.º 41/2004 em Diário da República: n.º 194, Série I-A, pp. 5241-5245.

A Lista Consolidada (LC) para a classificação e avaliação da informação pública, apresentada pela Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB), é um instrumento que contextualiza os diversos processos de negócio das entidades públicas e que pretende servir de referencial ao desenvolvimento de instrumentos organizacionais (ou pluriorganizacionias), para a classificação e avaliação da informação pública (DGLAB, 2021), face à fundamentação para a recolha, ao tratamento e à conservação dos dados. A LC também disponibiliza a definição do tempo, em termos da conservação dos dados e o destino final, bem como o apoio legal ou outro que justificam estas ações. Este instrumento adota uma organização hierárquica de classes que patenteiam: funções, subfunções e procedimentos de negócio desenvolvidos pela AP, incluindo a sua exposição e apreciação (DGLAB, 2021).

A GD ao implementar a norma ISO 26122, tem o objetivo de acompanhar o ciclo de vida integral de um documento, que pode assumir diferentes formas e é examinado de forma individual, desde a produção à preservação ou eliminação (Pinto, 2013).

O arquivo de documentos oficiais e a sua conversão eletrónica, desencadeou uma regulamentação adequada, dado que a sua origem e o seu acesso podem levantar questões, não só de natureza técnica, como jurídica, tanto em termos nacionais, como internacionais. No espectro das normas ISO, que materializam orientações relativamente aos documentos temos:

- a ISO 23081 (depósito de documentos)
- a ISO 13028 (digitalização)
- a ISO 27001 (segurança)
- a ISO 13008 (migração),

tarefas estas que são desenvolvidas pelo Sistema de Gestão Documental (SGD).

Em conciliação com esta disposição normativa, a OCDE (Cardoso, 2018) defende que o governo eletrónico conseguirá tirar partido das novas tecnologias, não só apenas com a desmaterialização de documentos, mas através da partilha de informação entre todas as organizações da AP, bem como entre a AP e os cidadãos.

A interoperabilidade é a faculdade que prevalece entre múltiplos sistemas que partilham e reutilizam informação, sem subsistir um custo de adaptação ou deterioração de significado associado (Agência para a Modernização Administrativa, 2011), sustentando desta forma um dos principais objetivos dos sistemas de informação. A evolução deste tipo de sistemas encontra-se interligada com a capacidade de certificação internacional destes sistemas de informação em Portugal, nomeadamente, com a transposição da norma ISO 26122, para a norma portuguesa.

Particularmente, a Diretiva 2003/98/EC desenvolve a questão da partilha de informação e o seu tratamento, para o setor público. Cabe neste caso à AP a responsabilidade de as organizações terem linguagens comuns, bem como uma taxonomia partilhada, garantindo desta forma uma integração entre sistemas. Enquanto a heterogeneidade nos sistemas informáticos empregues pela AP subsistir, prevalece a complexidade de transformar a informação, em conhecimento partilhado.

Em ambiente organizacional, o desenvolvimento de um SGD é associado a uma garantia de domínio de informação, bem como o seu acesso rápido. Segundo Shipman (1999) é visto como um sistema que controla: a conceção, o armazenamento, a partilha, a disponibilização e o método de atualização dos documentos. Aqui encontra-se também incluído o controlo do *check-in*, *check-out* e a revisão dos documentos. Posteriormente, a vertente informática de gestão que aporta a simplificação da manipulação documental é também incluída (Silva, 2000).

É importante que o SGD seja compatível com a estratégia da organização a nível interno e externo (Garcia-Alsina, 2012). A nível interno estão em causa: a estrutura, a cultura e as expetativas organizacionais, as políticas, normas e estatutos, os recursos, sistemas e fluxo de informação. Já a nível externo é importante a organização munir-se de informação sobre as seguintes vertentes onde se encontra inserida: social, cultural, legal, normas, financeira, tecnológica e económica. É também crucial a gestão de expetativas dos interessados, as exigências do negócio, a ética e as boas práticas (Garcia-Alsina, 2012).

A GD torna-se assim fulcral na gestão de documentos. Como características principais de um SGD temos:

- *Check-in/check-out* e bloqueio (de forma a permitir a edição sincronizada de um documento e que as modificações de um individuo não se sobreponham as de outro);
- Controlo das diferentes versões (hipótese de consultar as diferenças entre o documento atual e as versões anteriores em caso de necessidade);
- *Roll back* (possibilidade de "ativar" uma versão precedente na eventualidade de equívoco ou disponibilização prematura);
- Percurso auditável (possibilidade de reconstituir as diferentes evoluções do ciclo de vida do documento neste sistema e os utilizadores que estiveram em causa) e

- Permissão de executar anotações (AIIM, 2021).

O planeamento e desenvolvimento de um plano estratégico de um SGD, subdivide-se no seguinte conjunto de etapas inventariadas na NP 4438:2005:

- Uma pesquisa global preliminar da organização (missão, visão, objetivos estratégicos, estrutura, contexto legal, político e praticável e posições fortes e fracas);
- Um exame das atividades desenvolvidas (serviços, atividades, tramitação e circuitos de informação);
- Identificação de requisitos dos documentos;
- Valorização e exame dos sistemas presentes;
- Inventariação das estratégias adotadas para atingir as necessidades de administração de documentos;
- Desenho e implementação do sistema de arquivo;
- Controlo, alinhamento e revisão.

O plano estratégico atinge o seu fim com a implementação prática do SGD e, por conseguinte, é possível uma apreciação contínua que permite controlar erros e adotar melhorias. Para que este processo seja eficaz é indispensável esclarecer as responsabilidades, com o apoio da gestão de topo, através da definição de uma política de GD. Após a aprovação desta política é necessário que, seguidamente, ela seja reconhecida dentro da organização, por parte de todos os colaboradores. Torna-se, assim, possível uma gestão integrada do arquivo, onde estão incluídas todas as imposições práticas, tomando como referência o contexto normativo (António, 2009).

Transversal a todo este contexto temos os recursos necessários dentro de uma organização. Recurso é um conceito limitativo quando estamos a referir-nos a indivíduos, como parceiros da organização. Os RH podem ser repartidos em três níveis distintos (Chiavenato, 2007):

- Nível institucional da organização – gestão
- Nível intermediário – gestão e assessoria
- Nível operacional – técnicos, funcionários e trabalhadores.

Os RH são vistos como todos os indivíduos que ingressam, permanecem e participam numa organização, independentemente da sua hierarquia ou tarefas (Chiavenato, 2007, cit. por Gomes, 2017). Os RH sempre foram e tendem a continuar a serem vistos como o motor da competitividade, dentro de uma organização (Lourenço, 2021). O indivíduo certo para determinada função garante um

sistema produtivo eficiente, logo certifica a subsistência da própria organização. E para que esta complexa harmonia seja conseguida (organização *versus* pessoas) é importante que a gestão global seja competente e cuidadosa, justificando assim a importância da GRH.

A adoção das TIC pela AP, principalmente na área dos RH que conserva um grande volume de informação, veio otimizar o tratamento e a gestão de documentos, permitindo um acesso mais célere. A GD beneficia, assim, da automatização de processos, com o apoio de *softwares*. Esta nova realidade disponibiliza a informação num único local, facilitando a administração, interação e tratamento de dados. A referida automatização permitiu a desmaterialização de documentos, por exemplo de identificação dos funcionários, e viabilizou o uso de formulários que podem ser acedidos *online*.

Tendo em conta o explanado acerca da GD, torna-se de extrema importância o circuito documental, já que tudo começa no momento da receção de um documento e a forma como este é aceite determina o seu tratamento. O circuito documental é constituído pelas seguintes etapas:

Figura 18: Circuito documental

Fonte: Lopes, 2016, p. 17.

A AP vivencia, atualmente, uma era que exige uma maior eficiência e eficácia no tratamento de documentos/informação, por forma a prestar um melhor serviço aos seus utentes e, desta forma, harmonizar uma melhor comunicação. Consequentemente, obter uma maior aproximação ao cidadão.

Portanto, concordando com Pinto e Silva (2005), a GI incorpora a GD, o que a torna elementar em termos práticos nas organizações, subsistindo uma interligação umbilical entre o ciclo de vida informacional e a gestão de documentos e proteção de dados.

4. PROTEÇÃO DE DADOS NA DIVISÃO ADMINISTRATIVA E DE RECURSOS HUMANOS DA CÂMARA MUNICIPAL DE VIANA DO CASTELO

4.1 METODOLOGIA

O estudo de caso é apenas uma das muitas formas de elaborar uma investigação em Ciências Sociais (Yin, 2005). Trata-se de uma abordagem metodológica de investigação particularmente adequada quando necessitamos compreender, explorar ou descrever ocorrências e contextos complexos, onde estão concomitantemente envolvidos fatores distintos. Portanto, é "uma investigação empírica que investiga um fenómeno contemporâneo dentro do seu contexto da vida real, especialmente quando os limites entre o fenómeno e o contexto não estão claramente definidos" (Yin, 2005, p. 32).

Os estudos de caso podem ainda ser do tipo: exploratórios, descritivos ou explanatórios (Yin, 2010). Mais especificamente, o estudo exploratório vai além da mera exposição de dados, prosseguindo para a sua explicação (Otley & Berry, 1994). Este tipo de estudo de caso pode produzir uma interseção entre a explicação teórica e a descrição de dados, onde decorre um trabalho indutivo de generalizações a partir de observações, concebendo-se assim premissas teóricas com base nas quais, de forma dedutiva, se procura explicar outros fenómenos.

O estudo de caso é um método que se distingue por nos permitir compreender uma questão complexa e por poder acrescentar força ao que já é conhecido. Uma grande vantagem é a sua aplicabilidade a situações humanas, a conjunturas contemporâneas da vida real (Dooley, 2002).

Neste contexto, investigadores de várias matérias empregam o método de investigação de estudo de caso para desenvolver a teoria, para produzir nova teoria, para disputar ou contestar a teoria, para explicar uma situação, para fornecer uma base para aplicar soluções a situações, para explorar, ou descrever um objeto ou fenómeno (Dooley, 2002). Possibilita refletir e trabalhar o objeto científico em contexto real, usando múltiplas fontes de prova ou dados (quantitativos e qualitativos), por forma a abranger a complexidade de um caso específico que tem interesse em si mesmo: "el objetivo primordial del estudio de un caso no es la comprensión de otros. La primera obligación es comprender este caso" (Stake, 2007, p. 17, cit. por Gomes, 2016, p. 22).

Os estudos de caso, na sua essência, são considerados de natureza qualitativa. Esta perspetiva e a perspetiva quantitativa diferem em três aspetos: explicação e compreensão; função pessoal e impessoal do investigador e conhecimento descoberto e construído (Stake, 1999).

Na vertente do modelo qualitativo, na primeira distinção destacam-se as inter-relações reais. A segunda, dá ao investigador uma reflexão de investigação de campo, como por exemplo a observação, os juízos de valor e análise. E, por último, a investigação foca-se na lógica da construção do conhecimento e não na lógica da descoberta (Stake, 1999).

Neste contexto, o estudo de caso pode ser regido pela sucessão das seguintes etapas: recolha, análise e interpretação da informação dos métodos qualitativos, sendo o propósito da investigação um estudo intensivo de um ou alguns casos (Latorre *et al*., 2003; Meirinhos & Osório, 2010).

O estudo de caso eleito nesta investigação centra-se no contexto autárquico de um órgão público, mais concretamente na DARH da CMVC. O objetivo é analisar a prática e a conformidade na proteção de dados pessoais dos utentes e funcionários na AP, através da plataforma de Gestão Documental utilizada: *e-SigGov*. Neste sentido, revelou-se essencial executar algumas tarefas como:

- ✓ Proceder a uma análise do RGPD, para compreender quais os requisitos funcionais necessários para um SGD estar em conformidade;
- ✓ Levantamento da cadeia de procedimentos, finalidades e categorias especiais dos dados pessoais utilizados (na *e-SigGov*);
- ✓ Elaborar um guião e realizar uma entrevista.

Entre os instrumentos de recolha de informação encontra-se a entrevista individual, a qual tem uma mais-valia e perspetiva valiosa, uma vez que é uma das fontes de informação mais importantes nos estudos de caso (Yin, 2005). Esta fonte de informação é um excelente instrumento para recolher a multiplicidade de descrições e interpretações que os sujeitos possuem sobre a realidade. A entrevista torna-se, assim, o instrumento adequado para captar estas múltiplas realidades, na posse do investigador qualitativo (Stake, 1999; Meirinhos & Osório, 2010).

Para a elaboração do guião de entrevista, Júnior e Júnior (2011) reuniram algumas caraterísticas importantes como:

- ✓ Na formulação das perguntas é importante que estas sejam padronizadas, para que possam ser comparadas entre si;
- ✓ As perguntas devem ser claras;
- ✓ As perguntas devem ser ordenadas de forma lógica e fomentando o interesse;
- ✓ Através da introdução da entrevista o objetivo e a natureza do trabalho deverão ser claros para o entrevistado. É importante que este fique esclarecido o que é pretendido e o motivo da entrevista;

- ✓ O entrevistado deverá estar correlacionado face à sua própria formação, experiência e áreas de interesse;
- ✓ Por fim, é importante o "consentimento esclarecido" por parte do entrevistado.

A entrevista estruturada, com consentimento esclarecido, foi realizada à Chefe de Divisão da DARH, no dia 24 de fevereiro de 2022, uma vez que se trata de uma responsável de serviço e utilizadora diária da referida plataforma de GD, bem como por ter acesso ao *feedback* de todos os colaboradores. Procurou-se, assim, obter uma visão real deste serviço face à adaptabilidade da obrigatoriedade do RGPD no SGD. O guião da entrevista elaborado pode ser consultado no apêndice 1.

4.2 CARATERIZAÇÃO DA ENTIDADE

A Câmara Municipal de Viana do Castelo (CMVC) é um órgão executivo colegial, composto por: um presidente, um vice-presidente e vereadores, definindo e executando políticas que visam a defesa dos interesses e da satisfação das necessidades de toda a população local. Desta forma, promovem o desenvolvimento do município em todas as áreas (CMVC, 2021a).

Como visão a CMVC "pretende constituir-se como uma referência nacional na territorialização da intervenção social, na rentabilização dos recursos existentes, no incentivo à cooperação, à parceria e à co-responsabilização dos agentes locais" (CMVC, 2021a). E como valores suporta: Subsidiariedade, Integração, Articulação, Participação, Inovação e a Igualdade de género (CMVC, 2021a).

Quanto ao seu enquadramento legal, temos o Decreto-Lei nº 115/2006 e a Resolução de Conselho de Ministros 197/97. Este Decreto-Lei visa reforçar o papel da rede social em todo o país, constituindo um novo tipo de parceria entre entidades públicas e privadas e concertando as ações desenvolvidas pelos diferentes agentes locais, levando à otimização dos recursos endógenos e exógenos.

Na prossecução da Resolução do Conselho de Ministros nº 197/97 foi desenvolvida uma fase piloto desta medida de política social, agregando num primeiro momento 41 concelhos. Atualmente a rede social está implementada em 275 concelhos, em todo o território continental (DL nº 115/2006, de 14 de junho).

Quanto ao Sistema de Gestão da Qualidade (SGQ), a CMVC obteve a certificação em 2006, segundo o referencial NP EN ISO 9001:2000. Esta certificação foi reiterada nos serviços prestados pela DARH e pela Divisão de Licenciamento de Obras Particulares. Este Município reforçou o investimento,

alargando o âmbito de certificação ao Gabinete das TIC e acompanhou a atualização para a norma ISO 9001:2008, ambos em 2009 (CMVC, 2021b).

Da lista de serviços certificados até ao momento constam: Departamento de Administração Geral, Departamento de Ordenamento do Território e Ambiente, Divisão Jurídica, Divisão Financeira e de Desenvolvimento Económico, Divisão de Gestão Urbanística, Secção de Arquivo e Serviço de Atendimento ao Munícipe (CMVC, 2021b). Neste momento está em desenvolvimento o planeamento da extensão desta certificação, também aos serviços da Divisão de Recursos Naturais (CMVC, 2021b).

4.3 ENTREVISTA

A estrutura orgânica do Departamento de Administração Geral da CMVC pode ser consultada no apêndice 2. Apresenta-se, seguidamente, a informação recolhida sobre os procedimentos da DARH face à adaptabilidade ao RGPD, através da entrevista. Na DARH os processos que contêm dados pessoais e a sua finalidade de tratamento são:

Processos que contêm dados pessoais	**Finalidade de tratamento**
Processos de Concurso	Seleção de Pessoal e Recrutamento
Formação	Emissão de Certificados de Formação
Acumulação de Funções (ACUF)	Cumprimento de obrigações legais
Medicina no trabalho	Exames, relatórios médicos e fichas de aptidão
Acidentes de Serviço	Exames, relatórios médicos e fichas de aptidão
Penhoras	Cumprimento de obrigações legais
Trabalhador-Estudante	Assistir às aulas e fazer provas escritas
Abonos de família	Beneficiar de abonos para os descendentes
Relação de Assiduidade	Registo de entrada e saída dos trabalhadores para o controlo da assiduidade
Candidaturas Espontâneas e Candidaturas a estágios curriculares ou profissionais.	Promoção de estágios Curriculares ou Profissionais (PEPAL)

As **categorias especiais de dados pessoais** que constam nos processos da DARH são: Filiação Sindical, Dados Biométricos, Dados relativos à saúde, Condenações Penais e Infrações (sanções disciplinares) e Dados Genéticos.

Existem **seis procedimentos implementados** na DARH para cumprir o estipulado no **RGPD**. A Auditoria Inicial, o Relatório Analítico de conformidade, as Medidas corretivas, a Criação de Formulários específicos, a Formação e as Auditorias.

A DARH, para **garantir a licitude**, limita o tratamento de dados pessoais a determinadas situações. Entre elas temos:

a) Para efeitos de cumprimento de obrigações legais, ou seja, tratamento de dados pessoais no âmbito de uma obrigação legal como, por exemplo, na qualidade de entidade pagadora;
b) Para o exercício de funções de interesse público;
c) Para a execução de contrato;
d) Para o preenchimento dos formulários.

A plataforma ***e-SigGov*** é o **SGD** implementado na CMVC. Na plataforma os **dados pessoais registados** são: nome, data de nascimento, sexo, número do cartão de cidadão, nacionalidade, contribuinte, e-mail, telemóvel, morada, estado civil e filiação.

A **proteção de dados pessoais é garantida** pela ***e-SigGov*** através de passwords, controlo de acessos, possibilidade de o funcionário trabalhar em casa com documentos já digitalizados.

Toda a **documentação** e **atividades de tratamento** na DARH são **registadas** da seguinte forma: primeiro o documento chega em forma física, depois é digitalizado e posteriormente segue o circuito em formato digital.

A DARH possui **processos físicos** através do pedido inicial (requerimento ou formulário). Quanto aos **processos digitais,** contêm o pedido e todas as informações e despachos referentes ao procedimento em causa.

No que respeita aos **prazos de conservação da documentação**, embora a DARH ainda não esteja a fazer avaliação e eliminação de documentação aplica-se a Portaria n.º 412/2001, de 17 de abril, que aprovou o Regulamento Arquivístico para as Autarquias Locais, com as alterações introduzidas no anexo n.º 1 do Regulamento Arquivístico pela Portaria n.º 1253/2009, de 14 de outubro.

Atualmente, nesta fase inicial de adaptabilidade ao RGPD, **a CMVC ainda não possui EPD**.

Quanto aos **dados pessoais especiais ou sensíveis, estes ainda não se encontram identificados ou classificados**, uma vez que a plataforma ***e-SigGov*** ainda não permite controlar acessos por classificação, ou seja, ainda não consegue limitar o acesso a estes dados.

A CMVC encontra-se, de momento, na **primeira fase de realização de uma auditoria**, no âmbito da implementação do RGPD. O **objetivo principal** desta auditoria é **permitir verificar** (com evidências) **a eficácia das medidas implementadas** na área de **Recursos Humanos** e, se necessário, modificá-las para estarem em conformidade com o RGPD. O objetivo das auditorias é percebido como o fomentar da introdução de melhorias no serviço.

No que respeita às **funcionalidades** disponíveis na ***e-SigGov*** temos:

- Digitalização de documentos recebidos por correio, e-mail, entregas presenciais, e seguimento da sua circulação;
- Repositório Digital;
- Gestão de utilizadores e de perfis de confidencialidade;
- Facilidade de exportação / importação para outros sistemas.

4.4 *E-SigGOV* - CARATERIZAÇÃO E TRAMITAÇÃO DE PROCESSOS

Em 2008 foi criada a Comunidade Intermunicipal do Alto Minho (CIM Alto Minho) ao abrigo da Lei n.º 45/2008 de 27 de agosto, à semelhança com outras zonas geográficas em Portugal. Atualmente é regida pela Lei n.º 75/2013 e engloba os municípios: Arcos de Valdevez, Caminha, Melgaço, Monção, Paredes de Coura, Ponte da Barca, Ponte do Lima, Valença, Viana do Castelo e Vila Nova de Cerveira (Comunidade Intermunicipal do Alto Minho, 2021).

A CIM Alto Minho desenvolve vários projetos e atividades, entre eles temos um projeto de GD, tendo como principal finalidade o desenvolvimento de uma plataforma de registo e gestão, como por exemplo, de correspondência (recebida e expedida), integrando desta forma as mais-valias das novas tecnologias.

Em termos de desenvolvimento desta plataforma, foi selecionada por concurso público a empresa J. Canão, Lda., apresentando uma Unidade de Investigação e Desenvolvimento (I&D) com características de qualidade e inovação fortes, oferecendo atualizações e melhorias contínuas, adequadas aos objetivos e necessidades do projeto. Esta empresa, em conjunto com o Instituto

Politécnico de Viana do Castelo, outro elemento deste projeto, projetaram e desenvolveram a plataforma *e-SigGov*.

Concretamente, esta materializa-se através de um *software* de gestão de documentos que aporta a vantagem da organização dos documentos num sistema cronológico, com tempos e configurações de execução e acessos, em tempo real, tornando tangível a desmaterialização de processos. Incorporando a proteção de dados, esta plataforma permite também o cumprimento normativo de acesso à informação, eliminando acessos e partilhas indevidos e garantindo o cumprimento dos prazos processuais. A partir deste momento foi possível reunir todos os documentos administrativos no mesmo local, interligá-los sempre que necessário, independentemente da hora, respeitando as credenciais necessárias.

A implementação deste SGD foi um processo complexo, que requereu uma equipa multidisciplinar e o envolvimento de diferentes departamentos / serviços: Arquivo, Engenharia Informática, Direito e GRH, que precisam partilhar informação. Todas estas áreas são essenciais e complementares entre si, acreditando uma execução efetiva e funcional do SGD e uma adequação dos processos e procedimentos a ele associados. O Município de Viana do Castelo começou este projeto de GD com o objetivo de organizar a área da documentação, instituindo uma modernização dos seus serviços. Da mesma forma procurava-se equalizar as atividades e procedimentos, com a implementação de modelos padrão, para a tramitação do envio de documentos.

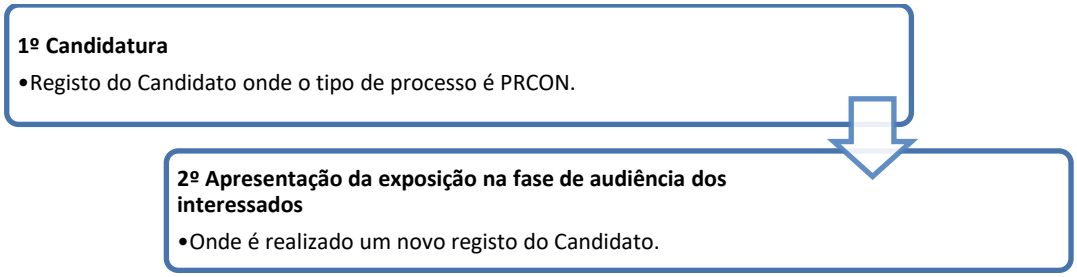
A plataforma *e-SigGov* é onde toda a documentação deve ser tratada, com o respetivo circuito associado. De uma maneira geral, todo o trabalho desenvolvido desde a sua estruturação prática demonstra um impacto positivo no Município. Diariamente, o trabalhador pode organizar as suas tarefas digitalmente, uma vez que consegue controlar a informação disponibilizada de forma centralizada, beneficiando principalmente da desmaterialização de documentos.

Expõe-se, de seguida, o "ciclo digital de um trabalhador", dentro da *e-SigGov*. Nesta plataforma, o documento padrão de identificação de um trabalhador é a "Ficha de Identidade", que contém: nome; morada; código postal, e-mail, telemóvel, cartão de cidadão, entre outros dados.

Procedimento Concursal (PRCON):

Os procedimentos de recrutamento e seleção de pessoal são regulados pela Portaria n.º 125-A/2019, que se encontra enquadrada na Lei n.º 35/2014 (Lei Geral do Trabalho em Funções Públicas).

Figura 19: Fases do Registo do Candidato, no Procedimento Concursal



Fonte: Elaboração própria.

Contratação do trabalhador

Para se iniciar este processo é necessário que exista uma bolsa de recrutamento, com uma lista da Categoria/Carreira e a respetiva graduação. Neste contexto, é iniciada uma "Informação Interna", apresentando a necessidade de contratação, a qual é registada através do Portal de Atendimento, ou seja, a plataforma *e-SigGov*.

Esta contratação compreende as três fases seguintes:

Fase 1 – Registo da informação interna

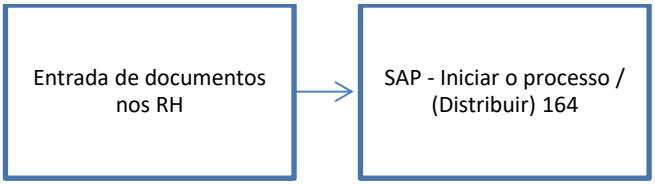
Após a submissão da informação pelo serviço requerente, já com o "Autorizo" do Vereador da área de RH, procede-se à consulta da bolsa de recrutamento para verificação do próximo candidato, pelo gestor do concurso, que informa a entrada de documentos do trabalhador com o seu nome e é feito o registo desta informação.

O registo da informação necessita:

- Palavra-chave: mencionar o nome do concurso que se pretende recrutar;
- "Documento Principal" do tipo de Informação necessidade recrutamento, que será classificado para o processo de candidatura do respetivo candidato.

O gestor do processo responsabiliza-se pelo suporte de papel. Após a classificação, o documento, segue o circuito que consta na figura seguinte.

Figura 20: Entrada de Documentos



Fonte: RH/PRCON.

É inserida, no RH/PRCON da candidatura do trabalhador, a informação necessária – tipo de documento: "Informação necessidade recrutamento". No decurso são gerados os seguintes documentos:

- Despacho de contratação (Despachos) – tipo: SAP > *Despacho de contratação*;
- Informação de cabimento (Informações) – tipo: SAP > *Informação cabimento*;
- Requisição externa (Documento Final) – tipo: *Requisição externa de despesa*;
- Ofício a solicitar o recrutamento (Ofícios) – tipo: SAP > *Ofício bolsa de recrutamento*.

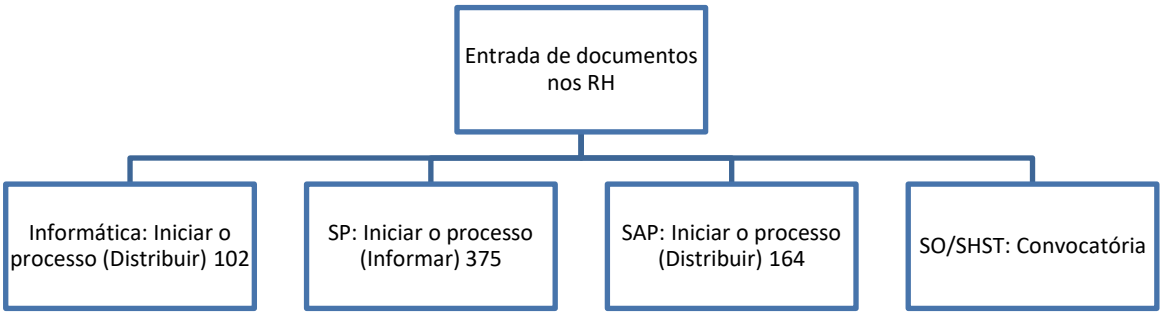
Fase 2 – Registo da documentação do novo trabalhador

É solicitada ao trabalhador a documentação necessária para a celebração do contrato. Quando esta é entregue, é submetida a entrada dos documentos nos RH e é solicitado à secção de processamentos o número mecanográfico do novo trabalhador. Consequentemente, é criada a sua Ficha de Cadastro (Anexo 1), gerando um processo do tipo TPF – Tipo de Processo de Funcionário, com os campos obrigatórios, nomeadamente:

- Nº de Mecanográfico – ano/número;
- Entidade;
- Nº de Contribuinte; Nº de Cartão de Cidadão; Telemóvel; Estado Civil;
- Unidade orgânica;
- Data Admissão.

Nos campos obrigatórios procura-se preencher todos os que se consiga obter através da documentação cedida, que posteriormente é digitalizada. Após a classificação e respetivo encaminhamento, deverão ser relacionados os processos existentes do trabalhador. Após a classificação, o documento segue o circuito da figura seguinte.

Figura 21: Circuito de documentação nos RH



Fonte: RH/PRCON.

Fase 3 – Entrega do relatório de período experimental

Na Fase 2 é entregue ao trabalhador um ofício, com o intuito de informar que dispõe de um prazo legal para apresentar um relatório do período experimental. Quando este relatório é recebido, é realizado o seu registo e conduzido para o respetivo gestor do processo. O ciclo do trabalhador perdura até à fase da sua Aposentação.

Processo Individual do Trabalhador – Documentos em Arquivo Físico/Cadastro Digital

No caso particular da CMVC, o processo individual do trabalhador é constituído pelo Arquivo e submetido pela DARH, mais especificamente pela Secção Administrativa de Pessoal. Este processo resume a vida laboral do trabalhador, bem como outros dados relevantes para o desempenho da atividade. Mais especificamente, integra um conjunto de documentos (provas) de natureza variada, consequente da relação jurídica de emprego público.

Os processos individuais dos trabalhadores admitem, em regra, documentos administrativos de caráter Não Nominativo (contrato de trabalho, certificados de formação e habilitações, registo de assiduidade, louvores), onde não subsiste reserva de acesso a dados. Comparativamente, os documentos Nominativos já são percecionados como “documentos administrativos” que abrangem os dados pessoais do trabalhador (dados genéticos, dados de saúde, dados reveladores da vida sexual, processos disciplinares, processos de penhoras, etc.), que ficam sujeitos aos termos normativos da proteção de dados pessoais.

O seu acesso é livre apenas por parte do titular dos respetivos dados, contudo um terceiro (alguém que não seja o próprio titular dos dados pessoais em causa) apenas pode proceder ao seu

acesso (tomar deles conhecimento) se: apresentar autorização escrita explicita, ou se lhe tiver sido reconhecido para o efeito um interesse direto, pessoal e legítimo.

O histórico laboral do trabalhador consta no seu processo individual. No caso particular da CMVC, o processo individual do trabalhador é realizado em formato físico (nome do trabalhador, nº mecanográfico e categoria), com uma lombada (nome e nº mecanográfico) e separadores, onde é organizada a informação, sem haver a diferenciação entre os documentos administrativos não nominativos e nominativos (ver Anexo 2).

Na GD do processo individual e, no decorrer do seu percurso profissional, o trabalhador pode ter vários tipos de processo (ver Anexo 3), onde constam os originais entregues, existindo posteriormente a sua digitalização para o cadastro (ver Anexo 1).

O cadastro digital e o processo individual do trabalhador são constituídos por diversos separadores/categorias, o que permite organizar toda a documentação referente especificamente ao indivíduo (ver Anexo 4). No processo documental estão digitalizados todos os documentos entregues pelo trabalhador e todos os documentos gerados para o tratamento do pedido (ofícios, despachos, informações, etc.).

4.5 TRATAMENTO DE DADOS PESSOAIS NO CONTEXTO LABORAL: REFLEXÃO

Conforme já exposto, o consentimento do titular dos dados apresenta-se como um dos trâmites de legitimidade previstos no processo de tratamento dos mesmos. Ou seja, cada finalidade de tratamento de dados equacionada é importante corresponder à necessidade de consentimento ou não, salvaguardando-se a licitude. Importa, assim, confrontar se há outro fundamento de legitimidade previsto pelo suporte legal (RGPD) para legitimar este tratamento.

Por exemplo, na DARH com o contrato de trabalho, a relação em contexto laboral implica uma recolha e tratamento de dados pessoais. Neste caso vigora uma disposição específica de tratamento como fundamento de legitimidade. Sendo assim, se a finalidade do tratamento de dados é uma relação laboral, então a gestão desses dados é regida pelo contrato de trabalho. Mas, se a finalidade do tratamento destes dados for além do necessário para executar o contrato, nesse caso é necessário o consentimento do titular para esse tratamento específico, com a finalidade de manter a licitude adequada.

Outra questão importante é o facto de o consentimento não ser idóneo, uma vez que o consentimento não será efetivamente livre (condição indispensável para a sua validade), devido ao

desequilíbrio da relação entre empregado e empregador, ou seja, sob supervisão e autoridade superior (CNPD, 2021b).

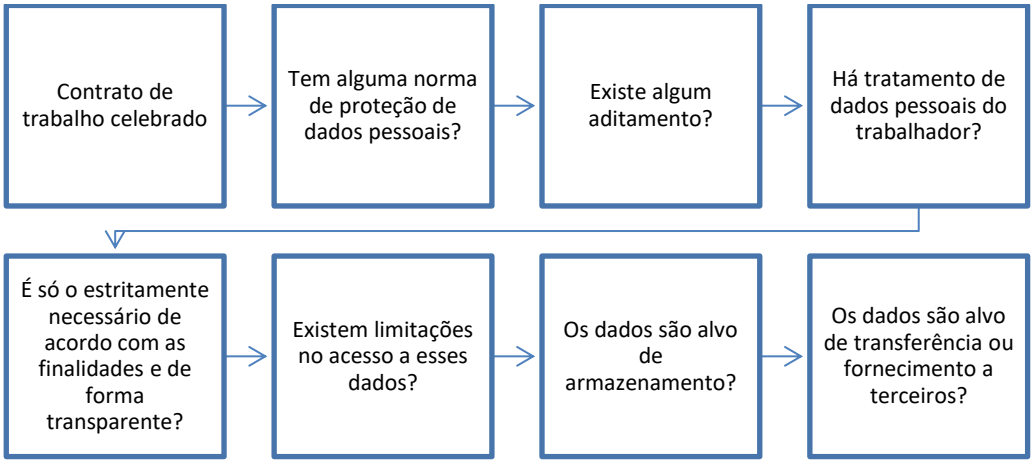
Portanto, no que respeita ao tratamento de dados pessoais em contexto laboral (art.º 88, RGPD - (UE) 2016/679) temos vários exemplos na DARH: recrutamento; recibos de vencimento; baixas médicas; formação profissional; celebração, execução e cessação de contratos; planeamento e gestão do trabalho; saúde e segurança no trabalho, entre outros. A proteção de dados pessoais aplica-se a: Trabalhadores (nacionais), Estagiários e Subcontratados.

Relembramos que no CT está salvaguardada a proteção dos dados pessoais e da vida privada, embora o RGPD tenha conduzido a uma proteção mais minuciosa do trabalhador, no momento do tratamento dos seus dados pessoais. Numa primeira instância, o empregado está mais protegido e o empregador necessita definir vários autodomínios, por forma a garantir que atinge todos os parâmetros, estabelecendo uma segurança mútua, de acordo com a legalidade. Segundo a Lei n.º 58/2019, de 8 de agosto:

> 1 - O empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo.
> 2 - O número anterior abrange igualmente o tratamento efetuado por subcontratante ou contabilista certificado em nome do empregador, para fins de gestão das relações laborais, desde que realizado ao abrigo de um contrato de prestação de serviços e sujeito a iguais garantias de sigilo.
> 3 - Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais:
> a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador (art.º 28., Lei n.º 58/2019).

Saldanha (2019), apresenta um conjunto alargado de controlos (cerca de 850) que fundamentam um suporte de trabalho, para que as organizações possam analisar ou ajustar procedimentos, bem como avaliar resultados com uma análise interna ou externa. Destacam-se alguns exemplos, em modo de perguntas:

Figura 22: Exemplos de controlos para as Organizações



Fonte: Adaptado de Saldanha (2019).

Do ponto de vista organizacional segundo Saldanha (2019), a primeira coisa a fazer neste processo é verificar se o contrato de trabalho realizado, possui alguma norma de proteção de dados pessoais dos trabalhadores. E, em caso negativo, se existe algum aditamento feito. Posteriormente confirmar se o tratamento de dados pessoais do empregado existe. Em caso afirmativo percebe-se se este é limitado ao estritamente essencial e face às finalidades, de um modo transparente. Depois é importante certificar se existem limitações no acesso a esses dados e por conseguinte, se estes são armazenados, transferidos ou fornecidos a terceiros.

Numa primeira instância, a DARH garante que o tratamento dos dados pessoais necessários para a realização do contrato de trabalho está estritamente justificado por essa mesma finalidade, garantindo assim a sua conformidade. Seguindo o circuito necessário do processo, ou seja, na continuação do tratamento, segue-se a digitalização dos documentos, para o seu posterior tratamento. Nesta etapa temos a introdução na via digital, através da plataforma *e-SigGov*, logo mantendo-se a conformidade.

Para garantir a licitude, a DARH limita ainda o tratamento de dados pessoais às seguintes situações: para efeitos de cumprimento de obrigações legais; para o exercício de funções de interesse público; para o preenchimento dos formulários e para a execução de contrato. Por fim, o acesso a estes dados pessoais é limitado através de *passwords* e controlos de acesso.

Neste contexto, Magalhães e Pereira (2018) introduzem o conceito de "*accountability*", que denota que as organizações se certificam que não há fugas de informação ou tratamento ilegítimo de dados. E ainda apresentarem a habilidade de provar que o regulamento é cumprido, por meio de

evidência em qualquer momento. O que requer também, segundo estas autoras, estruturar e executar políticas de "*data governance*", como instrumentos de conferência de conformidade, bem como a implementação de auditorias de autocontrolo contínuo e de avaliação da eficiência destes instrumentos.

Este princípio também aconselha, que a organização registe toda a documentação e atividades de tratamento (art.º 30, (UE) 2016/679), acautelando-se em matérias de segurança adequadas ao risco como, por exemplo, a pseudonimização.

A CMVC encontra-se de momento a realizar uma pré auditoria, através de uma empresa subcontratada, que permitirá ter acesso a dados concretos, sobre a eficácia das medidas implementadas até ao momento na DARH, o que também inclui a *e-SigGov*. Com este relatório será possível obter uma leitura clara da necessidade ou não de realizar alterações, com o intuito principal de garantir a conformidade com o RGPD. Na DARH as auditorias são percebidas, como uma medida importante na introdução de melhorias no serviço.

Todas as organizações (públicas ou privadas) têm a obrigação de prestar a sua colaboração à CNPD (art.º 8, Lei n.º 58/2019). E, em particular o art.º 33 da Lei n.º 58/2019, de 8 de agosto, determina a participação da violação dos dados ou *data breach*. Sempre que existir deteção de violação dos dados, seja por acesso indevido, fuga ou ciberataques, o responsável pelo tratamento deve comunicar à CNPD (prazo de 72 horas). Esta participação também deve ser feita ao titular dos dados, por representar um elevado risco para os seus direitos e liberdades (art.º 34, Lei 58/2019).

A CMVC nesta fase inicial de adaptabilidade ao RGPD, ainda não possui EPD. Um dos objetivos previstos após a obtenção dos resultados da pré auditoria, trata-se da obtenção de linhas orientadoras que permitam a implementação do órgão EPD.

Posto isto, com o objetivo de assegurar a segurança e limitar as violações de dados, Machado (2020, p. 28) avança com uma estratégia:

> 1. Identificação das fraquezas do sistema (de modo a ter perceção dos riscos) 2. Cálculo da probabilidade (mais provável a falha aquando da comunicação de dados e quando há recurso á subcontratação) e impacto de determinadas ameaças 3. Definição de medidas de segurança adequadas de acordo com a entidade em questão, face ao analisado anteriormente.

Um outro aspeto importante que deve ser referido é o caso das entidades subcontratadas. Estas, quando são contratadas para algum serviço pela organização principal, passam a ter responsabilidades acrescidas na execução do seu trabalho, visto passarem a ter contacto com um

conjunto de dados pessoais. Nestes casos, estas empresas passam a estar também abrangidas pelo RGPD, pois desenvolvem operações de tratamento de dados pessoais.

A CMVC, conforme já referido, encontra-se a realizar uma pré auditoria de avaliação, que permitirá obter valiosas elações da realidade atual do serviço e, posteriormente, fazer as adaptações necessárias que garantam a conformidade e licitude do tratamento de todos os dados pessoais a que tem acesso. A DARH neste momento, para além da limitação do número de pessoas que têm acesso a estes dados, minimizando a probabilidade de falha, também possui uma gestão rigorosa dos próprios acessos, delimitando igualmente estes acessos pelo tipo de serviço executado.

4.6 PROPOSTAS DE MELHORIA

A utilização das TIC exponencia uma maior capacidade de gestão de arquivos e difusão de documentos não só na GRH, como nos restantes setores da AP.

Seguidamente, reflete-se em termos práticos sobre o tratamento e proteção de dados pessoais na CMVC, mais especificamente na DARH. Enunciam-se, igualmente, algumas propostas de melhoria, que poderão ser equacionadas face à realidade interna do serviço.

Atualmente, a implementação da norma ISO 26122 na DARH tem como objetivo desenvolver a GD de acordo com dois critérios específicos:

1º Critério - Análise funcional do documento:

Cada função do documento deverá corresponder a um processo apenas, entendido no conceito de ação específica.

2º Critério - Análise sequencial do documento:

Existe a necessidade de verificação do fluxo da informação, ou seja, quais as necessidades de partilha, dentro da estrutura organizacional. Neste contexto, a aplicação da norma pressupôs um estudo prévio de processos de trabalho, recorrendo igualmente à desmaterialização de documentos. Através deste procedimento de digitalização, o trabalhador concederá toda a documentação oficial, incluindo documentos de identificação, certificados, etc.

3º Critério – aplicação da norma ISO 26122, no contexto *e-sigGov*:

Neste critério subsistiu a necessidade de garantir a aplicação da norma ISO 26122, na implementação da plataforma *e-sigGov.* Neste caso, é importante que exista a garantia de proteção de dados, durante o processo sequencial dos documentos.

Passa a estar garantido o acesso à documentação, apenas às entidades públicas que dele devem tomar conhecimento. Para este efeito, existe o sistema de adoção de *passwords*, que autorizam o fluxo entre entidades da AP. Este requisito foi facilmente ultrapassado, uma vez que já subsistia uma experiência de partilha de informação entre serviços da AP, informação que foi partilhada com os fornecedores de *software*.

Resumindo, a CMVC passou a oferecer:

1. **Garantia de confidencialidade**, ou seja, a certificação do *software* desenvolvido para os seus serviços, concede a garantia de que o documento original, acompanhará os circuitos adequados, segundo os critérios de confidencialidade.
2. **Procedimentos mais céleres e organizados**, através do processo de desmaterialização na DARH, em conciliação com a adoção de um sistema de base de dados.
3. **Comunicação integrada mais descomplicada**, através da simplificação da interoperabilidade semântica, que passa a possibilitar o contato direto, a troca de ofícios ou outros documentos/informações, com as entidades (AP ou entidades privadas).

Após a análise e explanação de todos os processos de tratamento de dados pessoais realizados na DARH da CMVC, constataram-se algumas dificuldades.

Um dos obstáculos presenciados refere-se ao facto de não existir um processo de *workflow* integrado, que essencialmente visa aumentar a eficiência da execução das tarefas.

Uma outra questão que se considera relevante, tem a ver com a impossibilidade de fechar o ciclo de um determinado procedimento administrativo, que neste caso teria resposta através da adoção de uma assinatura digital. Associando a obrigatoriedade da assinatura a determinado dirigente/executivo, determinados procedimentos (comunicações, certidões, declarações, etc.), poderiam ser realizados digitalmente. Por exemplo, salienta-se que com a intransmissibilidade do certificado digital ou cartão do cidadão é possível garantir a fiabilidade e confidencialidade deste procedimento. Ou seja, esta chancela (assinatura digital) dada a determinado conteúdo (documento ou e-mail) permite certificar que este não foi alterado, depois da sua aplicação. E, no seguimento desta informação, a entidade que rubricou digitalmente o documento, não pode contestar a sua veracidade. Neste contexto, também existe uma ligação à hora e data em que o documento foi assinado e enviado.

Por último, outro obstáculo é o facto de ainda não existir a submissão online, ou seja, o trabalhador ter a possibilidade de submeter todos os requerimentos que pretende, de forma digital.

Face ao explicitado, apresentam-se algumas propostas de melhoria a desenvolver pela **CMVC** e, por conseguinte, pela **DARH**.

- Sensibilizar e formar os colaboradores para o uso correto do email (Para, CC, Bcc) e das diferentes aplicações, e para a segurança informática em geral;

- Sensibilizar os colaboradores para as questões da privacidade e de responsabilidade profissional;

- Sensibilizar para a segurança da informação digital e não digital;

- Avaliar com a Qualidade e com os RH a possibilidade de promover ações de formação / sensibilização no âmbito dos procedimentos informáticos e processuais corretos e uniformizados;

- Implementar um processo uniformizado e integral de tratamento e gestão de documentos;

- Garantir o *login* exclusivo para cada colaborador em todas as aplicações;

- Avaliar o tratamento de dados pessoais sensíveis no âmbito dos diferentes processos, o tratamento de comunicações indevidamente dirigidas e de comunicações abusivas;

- Uniformizar as bases de dados dos cidadãos (1 registo para todas as aplicações);

- Avaliar a consulta de processos em papel;

- Desenvolver uma listagem dos prazos legais de conservação mínima e máxima dos dados (em papel e digital);

- Promover a desmaterialização em todos os processos;

- Implementar a instalação de dois monitores para colaboradores selecionados (facilita a desmaterialização);

- Implementar o pedido de consentimento para envio de divulgação em papel;

- Reavaliar e implementar um plano de segurança das instalações;

- Avaliar a integridade das aplicações produzidas internamente.

Especificamente para a ***e-SigGov***, apresentam-se algumas notas de melhoria:

- Promover a digitalização dos documentos e a codificação dos mesmos;

- Configurar todos os formulários online para incluir o consentimento / conhecimento da política de privacidade da CMVC;

- Implementar permissões de acesso por tipo de documento;

- Reavaliar e configurar o acesso dos diferentes colaboradores aos dados pessoais existentes, nas diferentes plataformas da forma mais aprimorada possível;

- Implementar processos digitais de pedidos de consulta de documentos, tanto externos como internos;

- Avaliar o desenvolvimento de um arquivo centralizado de documentos pessoais digitalizados dos colaboradores, com acesso restrito e justificado.

CONCLUSÃO

A Sociedade da Informação e o desenvolvimento tecnológico atual exigem dos cidadãos e do setor público e privado uma grande capacidade de adaptabilidade, apesar das dificuldades em termos técnicos e, por vezes, económicos.

A CI é caraterizada como uma "ciência social aplicada, de tipo trans e interdisciplinar, dotada de identidade própria e alicerçada num corpus teórico-metodológico consistente." Desta forma, a "CI resulta de uma dinâmica de integração do legado técnico e prático das tradicionais disciplinas ligadas à guarda e conservação dos documentos, legado esse essencial para o estudo científico do objeto informação" (Gomes, 2016, p. 285).

O atual posicionamento científico da CI é percebido como uma mais-valia no desenvolvimento desta investigação, principalmente em quatro aspetos: suplanta a compartimentação tradicional da informação (física e tecnológica); proporciona a análise e compreensão da produção informacional dinâmica; a sua retenção e utilização e, por fim, permite conhecer e compreender a informação na gestão de qualquer instituição (Gomes, 2016).

A nova realidade apresentada pelo RGPD capacita as entidades públicas, como o principal impulsionador quanto ao cumprimento das novas normas de proteção de dados, em coordenação com o setor privado, impondo-se a reflexão entre o tratamento de dados na sua operacionalidade e os sistemas de segurança de redes e informação empregues.

Especialmente na área dos RH, que conserva um grande volume de informação/documentos, as TIC na AP otimizaram a GD, de forma que esta beneficia da automatização de procedimentos que agilizam e mitigam funções, através do apoio de *softwares*, como a plataforma *e-SigGov*. É, assim, garantida a disponibilização da informação num único local e *online*, facilitando a administração, interação e o tratamento de dados. Este processo legítimo levado a cabo pela AP é garantido pelos princípios fundamentais de tratamento de dados pessoais estipulados no RGPD.

Neste contexto, impera a necessidade de a AP se manter atualizada, adotando uma metodologia de implementação capaz, em termos de conformidade, uma vez que o RGPD impõe uma análise e revisão exaustivas nestes tratamentos. Originando em veto ou permissão de acesso aos documentos administrativos nominativos, tendo em conta os critérios de proporcionalidade. Resultando, nestes casos, na partilha limitada de informação ao estritamente fundamental face à finalidade invocada, instituindo uma comunicação fracionada sempre que possível, suprimindo os dados pessoais que não sejam relevantes para determinado fim.

O papel do profissional da informação na GD foi sendo percebido e concretizado em ações e desempenho de funções concretas. Face a esta realidade da necessidade de adaptabilidade ao RGPD,

este papel considera-se indispensável, no âmbito do equilíbrio entre uma otimização dos procedimentos na AP, sem comprometer a licitude e a conformidade.

Resultante desta investigação profissional e pessoal, destacam-se algumas propostas de melhoria a implementar pela DARH e, por conseguinte, pela CMVC:

- Sensibilizar e formar os colaboradores para o uso correto das diferentes aplicações / plataformas e para a segurança informática, em geral;
- Informar e formar os colaboradores nas questões da privacidade, proteção de dados e de responsabilidade profissional;
- Sensibilizar para a segurança da informação digital e física.

Estas propostas de melhoria elencadas podem ser vistas como ponto de partida para qualquer organização, já que se referem ao cerne de muitas das questões suscitadas ao nível do tratamento de dados pessoais na prática profissional.

Estas propostas trarão uma maior compreensão entre a estrutura e ramificações do RGPD, por parte de todas as partes integrantes nos diferentes processos de tratamento de dados pessoais. Denote-se que, este universo transmite a inclusão da comunicação entre as diferentes instituições públicas, setor privado e particulares, não apenas numa divisão ou instituição.

No momento de conclusão deste estudo, as propostas de melhoria apontadas são relevantes, salientando-se a necessidade de flexibilidade face à mutação e volume de informação, ou seja, à medida que o trabalho esteja a ser desenvolvido porventura serão necessários vários ajustes práticos.

Em suma, foi bastante enriquecedora esta investigação em termos pessoais e profissionais, uma vez que permitiu uma análise e compreensão transversal da realidade vivida na CMVC e, mais especificamente, na DARH, já que subsistia um pré conhecimento do período anterior ao RGPD e, desta forma, acompanhou-se todo o trabalho realizado até ao momento face à adaptabilidade necessária.

Ressalvamos, igualmente, a valorização do percurso de investigação adotado, desde o estudo do quadro legislativo do RGPD (intracomunitário e português), conceitos e direitos no tratamento de dados pessoais na AP e a importância da GD neste cenário. Torna-se evidente a interdisciplinaridade que a temática em estudo exigiu e, não se restringiu à teoria, mas também ao conhecimento operacional.

O saber interdisciplinar adquirido neste ambiente académico, rico em grandes mentes e profissionais da CI, foi uma experiência incalculável em conhecimento, uma influência para um desempenho profissional mais capaz, confiante e responsável. Facto este que, todos os dias se torna mais evidente, uma vez que estas competências continuam a ser trabalhadas diariamente e sempre com o objetivo de fazer mais e melhor.

No que respeita à reflexão pessoal, o papel de profissional da informação é igualmente importante, uma vez que acompanha todas as fases do ciclo de vida do tratamento de dados pessoais na DARH, desde a sua entrada até ao seu arquivo. Fases do tratamento de dados pessoais como a entrada, a desmaterialização ou, até mesmo a eliminação de acordo com a legislação, são percebidas como extremamente sensíveis e relevantes na AP, uma vez que o controlo da limitação de acesso, por exemplo, é bastante importante. É indispensável que os processos administrativos sejam céleres, claros e simples, dado o fluxo diário de informação e, em face da sua necessidade de tratamento, independentemente da complexidade de adaptação ao RGPD.

A realidade da GD na AP é bastante complexa, uma vez que, por defeito, face à sua natureza pode ser inelástica. E, tendo em vista os seus objetivos, investe aos processos e aos profissionais da CI um grande peso, dada a necessidade de adaptação. Subsiste uma grande necessidade de leveza e clareza, em detrimento de procedimentos morosos e complexos.

Por fim, destacamos três condicionantes da realidade deste estudo: o desenvolvimento de uma atividade profissional, a tempo integral, no período desta investigação; o limite temporal disponível e o impacto físico e psicológico que as imposições da Covid-19 aportaram.

REFERÊNCIAS BIBLIOGRÁFICAS

Agência para a Modernização Administrativa (2011). *Interoperabilidade na administração pública: procedimentos para a adesão à iAP - Plataforma de Interoperabilidade da Administração Pública.* Versão 3.0. Lisboa: Agência para a Modernização Administrativa. https://1library.org/document/ydmx7vly-interoperabilidade-na-administracao-publica-procedimentos-para-adesao-a-iap-plataforma-de-interoperabilidade-da-administracao-publica.html

AIIM (2021). *What Is Document Management (DMS)?* https://www.aiim.org/what-is-document-imaging

António, R. (2009). *Desafios profissionais da Gestão Documental*. Edições Colibri. Lisboa

Associação para a Promoção e Desenvolvimento da Sociedade da Informação (2014). *O tratamento de dados pessoais em Portugal. Breve Guia prático.* PowerPoint Presentation (apdsi.pt)

Barros, A., Barbedo, F., Santos, G., Runa, L., Garcia, M., & Penteado, P. (2008). *Rede Portuguesa de Arquivos (RPA): fundamentos para o seu desenvolvimento e gestão - Módulo 2: modelo lógico*. Arquivos em Linha: DGARQ. https://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/rpa_ml1.pdf

Bilhim, J. (2004). *Gestão Estratégica de Recursos Humanos*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.

Butarelli, G. (2018). *Towards a digital ethics EDPS Ethics Advisory Group. REPORT 2018.* https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

Calderon, W., Cornelsen, J., Pavezi, N., & Lopes, M. (2004). O processo de gestão documental e da informação arquivística no ambiente universitário. *Ci. Inf.*. (33)3. 97-104. Revista-v33-n3-set_dez-2004.indb (scielo.br)

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

Câmara Municipal de Viana do Castelo (CMVC) (2021a). *Rede social*. http://www.cm-viana-castelo.pt/pt/rede-social

Câmara Municipal de Viana do Castelo (CMVC) (2021b). *Sistema de Gestão da Qualidade (SGQ)*. http://www.cm-viana-castelo.pt/pt/sistema-de-gestao-da-qualidade-sgq

Chiavenato, I. (2007). *Administración de recursos humanos: El capital humano de las organizaciones*. 8ª edição. McGraw-Hill.

Colaborador *DocuSign* (2021, Janeiro 11). 8 principais erros na gestão de documentos do RH. *Blog DocuSign*. https://www.docusign.com.br/blog/erros-na-gestao-de-documentos-do-rh

Comissão Europeia (2021). *Como deve ser solicitado o meu consentimento?* Como deve ser solicitado o meu consentimento? | Comissão Europeia (europa.eu)

Comissão Europeia (2021). *Quais são os principais aspetos do Regulamento Geral sobre a Proteção de Dados (RGPD) de que as administrações públicas devem estar cientes?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_pt

Comissão Nacional de Proteção de Dados (2017). *10 medidas para preparar a entrada em vigor do RGPD – Regulamento Europeu de Proteção de Dados*. (1-3). https://www.sg.pcm.gov.pt/media/33598/06.pdf

Comissão Nacional de Proteção de Dados (2021a). *O que somos e quem somos*. https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

Comissão Nacional de Proteção de Dados (2021b). *Áreas temáticas – Consentimento.* https://www.cnpd.pt/organizacoes/areas-tematicas/consentimento/

Comunidade Intermunicipal do Alto Minho (2021). *Quem somos*. http://www.cim-altominho.pt/gca/index.php?id=343

Conselho da UE e do Conselho Europeu (2020, Setembro 21). *Mercado único digital na Europa.* https://www.consilium.europa.eu/pt/policies/digital-single-market/#

Coreni, E. (2018). *Regulamento Geral de Proteção de Dados - O impacto Causado numa Organização*. Trabalho final de Mestrado. ISEG. https://www.repository.utl.pt/bitstream/10400.5/16675/1/DM-EC-2018.pdf

Cunha, D., Silva, D. & Hierro, A. (2020). *Guia do processo de adequação ao regulamento geral de proteção de dados. Implementação e auditoria.* 1ªed. Edições Almedina

Cunha, M., Rego, A.; Cunha, R., Cabral-Cardoso, C.; Marques, C.; e Gomes, J. (2010) *Manual de Gestão de Pessoas e do Capital Humano*. Edições Sílabo.

Dessler, G. (2003). *Administração de recursos humanos*. 2. ed. Tradução de Cecília Leão Oderich. São Paulo: Pearson Prentice Hall.

Pearson. https://cucjonline.com/biblioteca/files/original/0ee49930c54202fa9d631ebce4af2438.pdf

DGLAB (2020). *Mapas Conceptuais da Lista Consolidada*. https://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2020/12/MapasConceptuais_nov_2020.pdf

DGLAB (2021). *Lista Consolidada*. https://arquivos.dglab.gov.pt/programas-e-projectos/modernizacao-administrativa/macroestrutura-funcional-mef/lista-consolidada/

Dionísio, C. (2018). *O novo paradigma do Regulamento Geral de Proteção de Dados e o Impacto na Cloud*. Dissertação de Mestrado. Universidade Técnica de Lisboa.

Dooley, L. M. (2002). Case Study Research and Theory Building. *Advances in Developing Human Resources*, 4(3):335–354.

EUR-Lux. (2020). *Proteção de Dados Pessoais (a partir de 2018).* https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex%3A32016R0679

European Data Protetion Supervisor (2021). EDPS Homepage | European Data Protection Supervisor (europa.eu)

Fazendeiro, A. (2017). *Regulamento Geral Sobre a Proteção de Dados*. 1ª ed. Almedina. Coimbra.

Fernandes, D. M. (2015). O princípio da transparência administrativa: Mito ou Realidade? *Revista da Ordem dos Advogados*, janeiro – junho, (425–457).

Finkelstein, M., & Finkelstein, C. (2019). Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileira*, 9(23), 284-301.

Francisco, S., & Francisco, D. (2019). Re*gulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública*. Edições Sílabo.

Freitas, C. (2020). *A Proteção de Dados Pessoais na Era Digital: A Evolução no Mundo e sua Previsão no Brasil*. [Seminar Presentation]. ETIC – Encontro de Iniciação Científica. 6(16). Toledo. http://intertemas.toledoprudente.edu.br/index.php/ETIC/index

Garcia-Alsina, M. (2012). Contribución de la serie ISO 30300 a la gestión de la documentación judicial. *Ibersid: Revista De Sistemas De Información Y Documentación,* 6, 135-143. https://www.ibersid.eu/ojs/index.php/ibersid/article/view/3991

Gomes, L. (2016). *Gestão da Informação, holística e sistémica, no campo da Ciência da Informação: estudo de aplicação para a construção do conhecimento na Universidade de Coimbra*. Tese de doutoramento. Universidade da Corunha. http://ruc.udc.es/dspace/handle/2183/18287 ; https://estudogeral.sib.uc.pt/handle/10316/43201

Gomes, T. D. G. (2017). *A influência da gestão de recursos humanos na motivação dos colaboradores*. Dissertação de Mestrado. Instituto Superior de Contabilidade e Administração do Porto. https://recipp.ipp.pt/bitstream/10400.22/10956/1/Tania_Gomes_MA_2017.pdf

Gouveia, J. B. (2015). Os Direitos Fundamentais na Constituição Portuguesa de 1976. *Revista Direito UFMS*. Edição Especial, 35-85. https://doi.org/10.21671/rdufms.v1i1.1233

Gouveia, L. (2017). *Notas e transparências sobre conceitos de Segurança da Informação e Proteção de Dados.* [Seminar Presentation]. Os conceitos de segurança da informação e proteção de dados. Versão 3.7. Universidade Fernando Pessoa. https://bdigital.ufp.pt/handle/10284/10340

Grisoto, R., Sant´Ana, J. & Segundo, J. (2015). A questão da privacidade no contexto da Ciência da Informação: uma análise das Teses e Dissertações de Pós-Graduação em Ciência da Informação da UNESP. *Revista Ibero-Americana de Ciência da Informação*, 8(2), 165–181.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2017, Abril 5). *Orientações sobre os encarregados da proteção de dados (EPD)*. WP 243 rev.01. wp243_rev.01_pt (cnpd.pt)

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2017, Outubro 4). *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*. WP 248 rev.01. wp248 rev.01_pt (cnpd.pt)

Instituto dos Arquivos Nacionais & Torre de Tombo. (2016). *Guia para a elaboração de cadernos de encargos e avaliação de software de sistemas eletrónicos de gestão de arquivos*. IAN/TT. Microsoft Word - GuiaSEGA_v1.0.doc (dglab.gov.pt)

Instituto dos Arquivos Nacionais & Torre de Tombo & Gabinete de Estudos de Arquivos Correntes (GEAC). (2005, Junho 2). *Apresentação da Norma NP 4438: Conteúdo e estrutura*. Lisboa

International Organization for Standardization. (2021). ISO - About us

Iramina, A. (2020). RGPD v. LGPD: Adoção Estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações.* 12(2). 91-117

Júnior, A. & Júnior, N. (2011). A utilização da técnica da entrevista em trabalhos científicos. *Evidência*. 7(7). 237-250. https://met2entrevista.webnode.pt/_files/200000032-64776656e5/200-752-1-PB.pdf

Lambert, P. (2017). *The Data Protection Officer*. 1st ed. Taylor & Francis Group.

Lares, A. & Karen C. (2005). *Tecnologías de Información en los Negocios*.5ª ed. McGraw-Hill. https://www.academia.edu/34613505/Tecnolog%C3%ADas_de_Informaci%C3%B3n_en_los_Negocios_5ta_Edici%C3%B3n_Daniel_Cohen_Karen_and_Enrique_As%C3%ADn_Lares_pdf

Lopes, A. (2016). *Circuitos Documentais e Gestão Documental: a necessidade de boas práticas arquivísticas*. Dissertação de Mestrado. Universidade da Beira Interior. uBibliorum: Circuitos Documentais e Gestão Documental: a necessidade de boas práticas arquivísticas

Lourenço, A., Penteado, P. & Barros, A. (2012). *Orientações para a Gestão de documentos de arquivo no contexto de uma reestruturação da Administração Central do Estado*. 2ª edição. DGARQ.

Lourenço, A., Penteado, P. & Gago, R. (2018). *A Lista Consolidada como instrumento facilitador de aplicação do RGPD*. [Journey presentation]. II Jornadas Gestão de Informação – Interação entre arquivistas e informáticos. https://eventos.bad.pt/wp-content/uploads/2018/01/P.-Barca_LC_CLAV_RGPD_v2.pdf

Lourenço, F. (2021). *Textos de Apoio de Gestão*. ESTSetúbal. 1-19. http://ltodi.est.ips.pt/pagsacec/Documentos/Gestao-EIG/EC_GEST_GRH_DOCUMENTA%C3%87%C3%83O_LP.pdf

Machado, F. (2020). *RGPD: conhecimento e impacto das organizações*. Dissertação de Mestrado. Instituto Superior de Contabilidade e Administração do Porto (ISCAP)

Magalhães, F. (2018). *Formação: Regulamento Geral de Proteção de Dados.* Ordem dos Contabilistas Certificados. https://www.occ.pt/fotos/editor2/rgpd-fmagalhaesmanual.pdf

Meirinhos, M. & Osório, A. (2010). O estudo de caso como estratégia de investigação em educação. *Eduser*. 2(2). 49-65. modelo_pdf-B2_2 (ipb.pt)

Mendes, S. L. (2014). *Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental*. Saraiva. São Paulo. https://books.google.com.br/books?hl=pt-PT&lr=&id=EDpnDwAAQBAJ&oi=fnd&pg=PT2&dq=prote%C3%A7%C3%A3o+de+dados+&ots=t6SLhIlyl8&sig=sTsfqHd6S-yrQvE2cozd1pdKB5E#v=onepage&q=prote%C3%A7%C3%A3o%20de%20dados&f=false

Moreira, T. (2017) Algumas implicações laborais do regulamento geral de proteção de dados pessoais no trabalho 4.0, *Questões Laborais*. Edições Almedina, S.A

Moreira, T. (2018). *O impacto do regulamento geral de proteção de dados nas organizações: um novo paradigma*. Dissertação de Mestrado. Instituto Superior de Contabilidade e Administração de Coimbra.

Mota J., e Sampaio A. P. (2019) Portugal - Regulamento Geral de Proteção de Dados em Portugal – Alguns Apontamentos à sua Lei de Execução. *Actualidad Jurídica Uría Menéndez*.53. (142-148). https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341

Nguyen, L. T., Swatman, P. & Fraunholz, B. (2007, Dezembro 5-7). *EDMS, ERMS, ECMS or EDRMS: Fighting through the acronyms towards a strategy for effective corporate Records Management* [Paper presentation]. Proceedings of the 18th Australasian Conference on Information Systems. Toowoomba. Austrália. https://www.researchgate.net/publication/239612319_EDMS_ERMS_ECMS_or_EDRMS_Fighting_through_the_acronyms_towards_a_strategy_for_effective_corporate_records_management

Oliveira, A., Motta, D., Melo, H. & Esteves, R. (2020). Empoderamento digital, proteção de dados e LGPD. *Pesquisa Brasileira em Ciência da Informação e Biblioteconomia*. 15(3). 247-261

Oliveira, D. (2009). *A relação entre a gestão de recursos humanos e o desempenho financeiro: um estudo multicasos no setor sucroalcooleiro*. Dissertação de Mestrado. Universidade de São Paulo. (Microsoft Word - Disserta\347\343o Denis Oliveira) (usp.br)

Otley, D. & Berry, A. (1994) Case study research in management accounting and control. *Management Accounting Research*. 5(1). 45-65.

Pais, A .(2021). O RGPD e as Organizações. [Webinar]. *RGPD para os Cidadãos e Organizações*. https://www.cim-regiaodecoimbra.pt/europe-direct-regiao-de-coimbra-promove-webinar-sobre-rgpd-para-os-cidadaos-e-organizacoes/

Penteado, P. (2018). O RGPD na Administração Pública: Perspetiva de gestão da informação arquivística. In *Gestão da informação, arquivos e proteção de dados: uma relação intrínseca.*

Ponta Delgada. http://repap.ina.pt/bitstream/10782/681/1/PPenteado-RGPF-GI_A%C3%A7ores_Jun2018.pdf

Pereira, J. (2018). *Controlo de contas e transformação da administração pública*. Fundação Demócrito Rocha | Universidade aberta do Nordeste. 10. 147-159. https://www.tce.ce.gov.br/downloads/Controle_Cidadao/f10_-_controle_cidadao.pdf

Pinheiro, A. S. (2016). A protecção de dados no novo Código do Procedimento Administrativo. Em Gomes, C., Neves, A. e Serrão, T., *Comentários ao novo Código do Procedimento Administrativo: I*. 339–366. AAFDL Editora.

Pinheiro, P. (2018). *Proteção de Dados Pessoais: Comentários à Lei N. 13.709/2018*. 2ª ed. Saraiva. https://books.google.com.br/books?hl=pt-PT&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT13&dq=prote%C3%A7%C3%A3o+de+dados+&ots=k8-lHpHR_O&sig=_6w08Uk46VXKpRojXAUWAO37eI8#v=onepage&q=prote%C3%A7%C3%A3o%20de%20dados&f=false

Pinto, A. (2018). *Gestão Documental e de processos na implementação do Regulamento Geral de Proteção de Dados (RGPD): O caso iPortalDoc.* Dissertação de Mestrado. Faculdade de Engenharia da Universidade do Porto. https://repositorio-aberto.up.pt/handle/10216/114164?mode=full

Pinto, M. & Silva, A. (2005). Um modelo sistémico e integral de Gestão da Informação nas organizações. In CONTECSI – 2.º *Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação* (pp. 1-24). https://repositorio-aberto.up.pt/bitstream/10216/13461/2/73495.pdf

Pinto, M. (2013). Gestão de Documentos e meio digital: um posicionamento urgente e estratégico. In *3.º Seminário de Estudos da Informação* (pp. 1-31). https://repositorio-aberto.up.pt/bitstream/10216/70837/2/77026.pdf

Portal dos Serviços Públicos (2021). *O que é o consentimento informado*. Consentimento informado - ePortugal.gov.pt

Presidência do Conselho de Ministros (2021). *Regulamento Geral de Proteção de Dados Pessoais (RGPD) - Proposta de plano de ação em 5 fases*. 04.pdf (pcm.gov.pt)

Saldanha, N. (2019). *RGPD Guia para uma auditoria de conformidade*. FCA.

Secretaria-Geral da Presidência do Conselho de Ministros (2018). *Orientações Práticas para a Administração Pública sobre o Regulamento Geral de Proteção de Dados (RGPD)*. https://www.sg.pcm.gov.pt/media/33595/05.pdf

Shipman, D. (1999). *EDM- Systems Ease Document Overload*. Document Management

Silva, J. (2000). *Gestão documental do processo de admissão de pessoal na administração* pública. Dissertação de Mestrado. Faculdade de Engenharia da Universidade do Porto. https://repositorio-aberto.up.pt/handle/10216/11080?mode=full

Stake, R. E. (2005) Qualitative Case Studies. In Denzin, N. K. & Lincoln, Y. S. (Eds.), *The Sage Handbook of Qualitative Research*. 3rd Edition. London: Sage Publications. pp. 443-466.

Stake, R. E. (1994). Case Studies. In N. Denzin & Y. Lincoln, *Handbook of qualitative research*. Newsbury Park: Sage. pp. 236-247.

Tavares, A. (2019). *Administração pública portuguesa*. Fundação Francisco Manuel dos Santos. https://books.google.com.br/books?hl=pt-PT&lr=&id=uKaODwAAQBAJ&oi=fnd&pg=PT2&dq=Administra%C3%A7%C3%A3o+P%C3%BAblica+&ots=NmO6cStbyq&sig=IchVoxJiZhQoBnoWRZ9etdeC0Vw#v=onepage&q=Administra%C3%A7%C3%A3o%20P%C3%BAblica&f=false

Teves, D. M. (2019). *A proteção de dados pessoais – o novo paradigma jurídico*. Dissertação de Mestrado. Faculdade de Economia e Gestão - Universidade dos Açores.

Universidade de Coimbra (2021). *Informação Administrativa e Proteção de Dados*. https://www.uc.pt/protecao-de-dados/perguntas_frequentes#q1

Vaz, A. (2018). *O Regulamento Geral de Proteção de Dados: Desafios e Impactos*. Dissertação de Mestrado. Faculdade de Direito da Universidade de Coimbra - FDUC. https://eg.uc.pt/bitstream/10316/85758/1/Disserta%C3%A7%C3%A3o.pdf

Vieira, F. (2018). *RGPD para cidadãos atentos: manual de curso online*. Lisboa: Instituto Nacional de Administração, I.P.

Vieira, T. (2007). *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.* Dissertação de Mestrado. Universidade de Brasília. *https://repositorio.unb.br/handle/10482/3358*

Vitorino, M. (2018). *Regulamento geral de Proteção de Dados: Impacto na Administração Pública*. Macedo Vitorino & Associados. https://www.macedovitorino.com/xms/files/2018/20181030-O_Impacto_do_RGPD_na_Administracao_Publica.pdf

Webster, B., Hare, C. & McLeod, J. (1999). Records management practices in small and medium sized enterprises: a study in North East England. *Journal of Information Science*. 25 (4). 283-294. Records management practices in small and medium sized enterprises: a study in North East England. - Northumbria Research Link

Yin, R. (2005) *Estudos de Caso: Planejamento e Métodos*, Porto Alegre: Bookman.

Legislação

Acórdão n.º 128/92 do Tribunal Constitucional. (1992). Processo: n.º 260/90. http://www.tribunalconstitucional.pt/tc/acordaos/19920128.html

Carta dos Direitos Fundamentais da União Europeia. (2016). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR

Constituição da República Portuguesa. (2015). (1-91). Constituição da República Potuguesa (parlamento.pt)

Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares. (1981). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

Convenção Europeia dos Direitos do Homem. (2021). Tribunal Europeu dos Direitos do Homem. https://www.echr.coe.int/documents/convention_por.pdf

Decisão-Quadro 2008/977/JAI. (2008). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0977

Declaração Universal dos Direitos do Homem (1948). Diário da República Eletrónico. https://dre.pt/declaracao-universal-dos-direitos-humanos

Decreto-lei n.º 4/2015 da Procuradoria-Geral Distrital de Lisboa (PGAR). (2015). Código do Procedimento Administrativo (versão atualizada). ::: DL n.º 4/2015, de 07 de Janeiro (pgdlisboa.pt)

Decreto-lei nº 115/2006 do Ministério do Trabalho e da Solidariedade Social (2006). Diário da República n.º 114/2006, Série I-A. 4276–4282. https://dre.pt/dre/detalhe/decreto-lei/115-2006-344943

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (2002). Jornal Oficial das Comunidades Europeias. https://www.uc.pt/protecao-de-dados/legis/20020712_diretiva_2002_58_ce_do_parlamento_europeu_e_do_conselho

Diretiva 2003/98/CE do Parlamento Europeu e do Conselho (2003). Jornal Oficial da União Europeia. L 345/90. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:pt:PDF

Diretiva 2006/24/CE do Parlamento Europeu e do Conselho. (2006). Jornal Oficial da União Europeia, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024&from=FI

Diretiva 95/45/CE do Parlamento Europeu e do Conselho (1995). Jornal Oficial das Comunidades Europeias. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:01995L0045-20060410&from=FR

Diretiva 95/46/CE do Parlamento Europeu e do Conselho. (1995). Jornal Oficial das Comunidades Europeias. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

ISO/IEC 13008 (2012). *Information and documentation — Digital records conversion and migration process.* Geneva. ISO

ISO/IEC 13028 (2010). *Information and documentation guidelines for digitization of records.* Geneva. ISO

ISO/IEC 23081 (2009). *Managing metadata for records*. Geneva. ISO

ISO/IEC 26122 (2008). *Information and documentation — Work process analysis for records - Part 1.* Geneva. ISO

ISO/IEC 26122 (2014). - *Electronic document management - Vocabulary - Part 2: Workflow management.* Geneva. ISO

ISO/IEC 27001 (2013). *Information security management systems*. Geneva. ISO.

ISO/IEC 27001:2013. (2013). International Organization for Standardization. ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27005:2011. (2011). International Organization for Standardization. ISO - ISO/IEC 27005:2011 - Information technology — Security techniques — Information security risk management

ISO/IEC 29100:2011, International Organization for Standardization. ISO/IEC 29100:2011(en), Information technology — Security techniques — Privacy framework

ISO/IEC 29134:2017. (2011). International Organization for Standardization. ISO/IEC 29134:2017(en), Information technology — Security techniques — Guidelines for privacy impact assessment

Lei n.º 26/2016 da Assembleia da República. (2016). Diário da República n.º 160, I série. (2777 – 2788). Lei n.º 26/2016 | DRE

Lei n.º 59/2019 da Assembleia da República. (2019). Diário da República, I série. (41-68). 20190808_lei_59_2019_prevencao_dtecao_investigacao_ou_repressao_de_infracoes (uc.pt)

Lei nº 43/2004 da Assembleia da República. (2004). Diário da República — I série -A. (5251- 5257). 52515257.pdf (dre.pt)

Lei nº 67/98 da Assembleia da República. (1998). Diário da República — I série -A. Nº 247. (5536- 5546). https://files.dre.pt/1s/1998/10/247a00/55365546.pdf

Parecer 4/2007 do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (2007). 12251/03/EN (gpdp.gov.mo)

Proposta de Lei n.º 120/XIII. (2018). Presidência do Conselho de Ministros. II série A. nº 89. (30- 48). https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

Recomendação n.º 9/A/2006 do Provedor de Justiça. (2006). Processo n.º R-3212/05. 009A_06.pdf (provedor-jus.pt)

Regulamento (CE) 2001/45 do Parlamento Europeu e do Conselho (2001). Jornal Oficial das Comunidades Europeias. https://op.europa.eu/pt/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-pt

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. (2016). Jornal Oficial da União Europeia. EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)

Regulamento (UE) 2016/680 do Parlamento Europeu e do Conselho. (2016). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680

Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho. (2018). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725

Texto de substituição da Proposta de Lei n.º 120/XIII/3.ª da Assembleia da República. (2019). Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias. (1-67). https://www.itinsight.pt/file/uploads/a8057c9320b07d31b96005aeb2ffebf1.pdf

Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia. (2007). Jornal Oficial da União Europeia. 2007/C 306/01. (1- 231). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=PT

Tratado de Roma que institui a Comunidade Económica Europeia (1957), CEE, https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/treaty-of-rome

Tratado sobre o Funcionamento da União Europeia (versão consolidada). (2016) Jornal Oficial da União Europeia. C 202. (47- 199). Tratado sobre o Funcionamento da União Europeia (versão consolidada) (europa.eu)

APÊNDICES E ANEXOS

APÊNDICE 1: Guião de entrevista

Este instrumento destina-se à recolha de dados, no âmbito da dissertação de Mestrado em Ciência da Informação em curso na Faculdade de Letras da Universidade de Coimbra.

1. Na DARH, identifique os processos que contêm dados pessoais.
2. Na DARH, quais as finalidades destes processos.
3. Identifique as categorias especiais de dados pessoais que constam nos processos.
4. Explique, no geral, quais os procedimentos implementados para cumprir o estipulado no Regulamento Geral sobre a Proteção de Dados (RGPD).
5. O tratamento de dados pessoais só é lícito em determinadas situações. Pode indicar como é realizado o seu tratamento lícito.
6. Na plataforma *e-SigGov* que dados pessoais são registados?
7. Na plataforma e-SigGov como é garantida a proteção de dados pessoais?
8. Como é realizado o registo de toda a documentação na DARH e atividades de tratamento?
9. Na DARH têm processos físicos e digitais? Arquivo físico e digital?
10. No que respeita aos prazos de conservação da documentação, qual a portaria utilizada?
11. Existe Encarregado de Proteção de Dados (EPD), na Câmara Municipal de Viana do Castelo (CMVC)?
12. Na CMVC, os dados pessoais especiais ou sensíveis estão identificados/classificados?
13. Na CMVC realizam auditorias? Com que objetivos?
14. A CMVC dispõe de um Sistema de Gestão Documental? Sim ou Não? Em caso afirmativo, qual o programa utilizado e o fornecedor?
15. Que funcionalidades estão disponíveis no Sistema de Gestão Documental?

Notas:

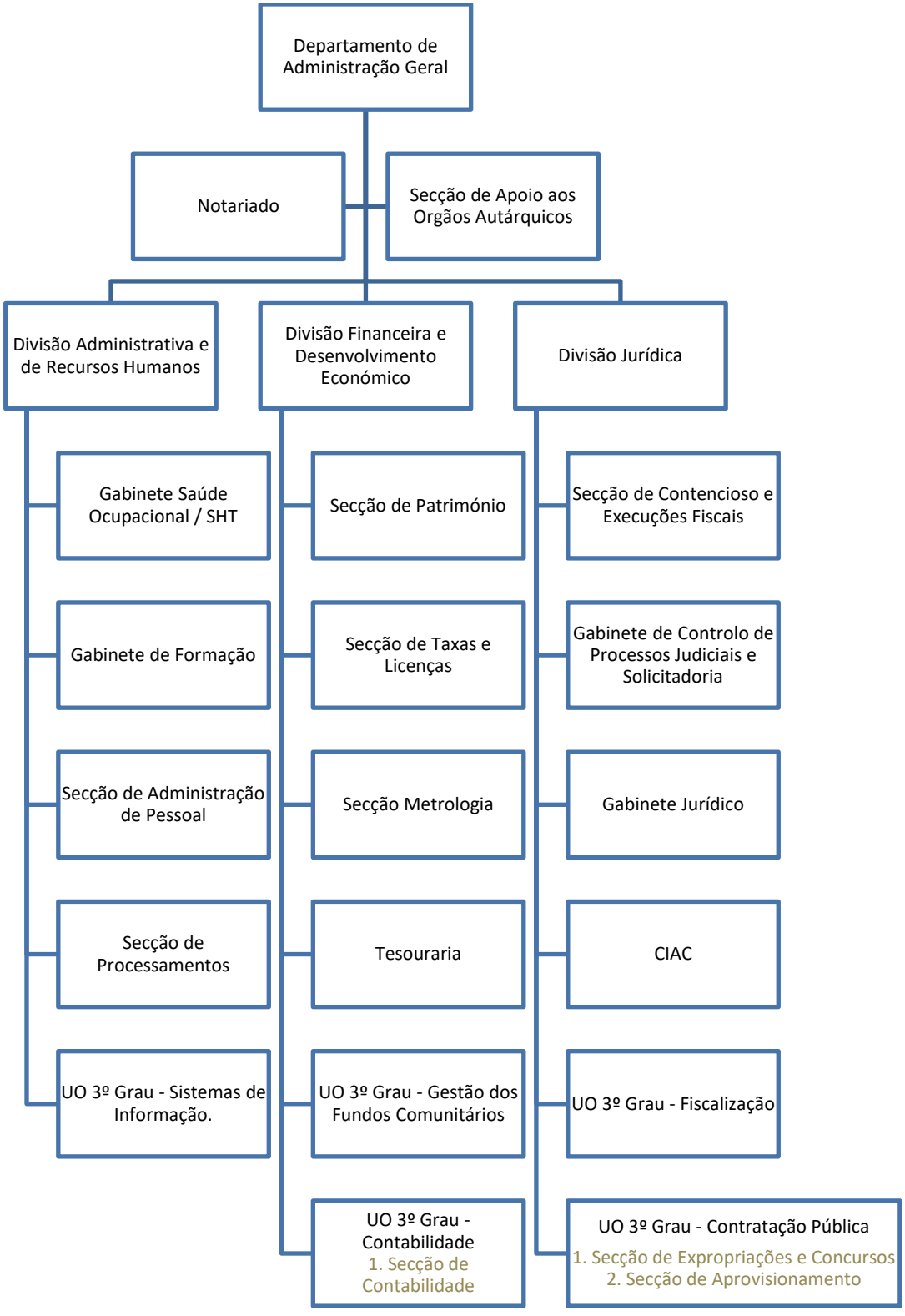
Dados Pessoais: "Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, 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" (art.º 4.º, n.º 1 do Regulamento (UE) 2016/679).

Categorias especiais de Dados Pessoais: dados "que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa "(art.º 9, nº 1, do Regulamento (UE) 2016/679).

Princípio da licitude e da lealdade: "objeto de um tratamento lícito e leal" (art.º 6, n.º 1, a), Lei 59/2019)

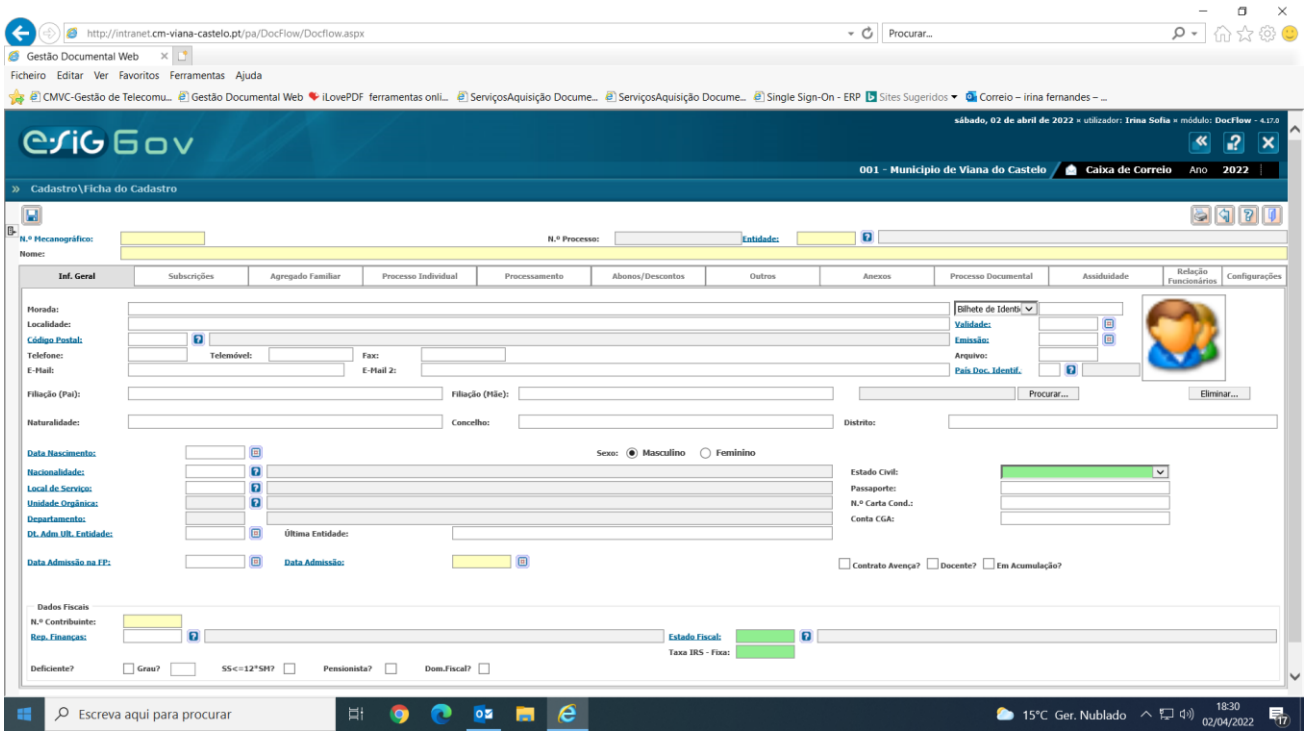
Consentimento: "Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (art.º 4.º, n.º 11 do Regulamento (UE) 2016/679)

APÊNDICE 2: Organograma do Departamento Administração Geral da CMVC



Fonte: Adaptação própria, após consulta do "Regulamento da organização dos serviços Municipais — Estrutura Flexível" e respetivas alterações, disponível em: http://www.cm-viana-castelo.pt/pt/regulamentos

ANEXO 1: Cadastro do funcionário



Fonte: DARH da CMVC.

ANEXO 2: Índice do Processo Individual

1. Situação Profissional
2. Dados Biográficos
3. Formação Profissional
4. Classificação de Serviço
5. Assiduidade ao Serviço
6. Habilitações Literárias
7. Subscrições Obrigatórias
8. Subscrições Facultativas
9. Fichas de Aptidão
10. Juntas Médicas
11. Acidentes de Serviço
12. Penalidades Disciplinares/ Penhoras
13. Exonerações ou Aposentações
14. Abonos/ Prestações Familiares
15. Trabalhador-Estudante
16. Declarações
17. Assuntos Gerais

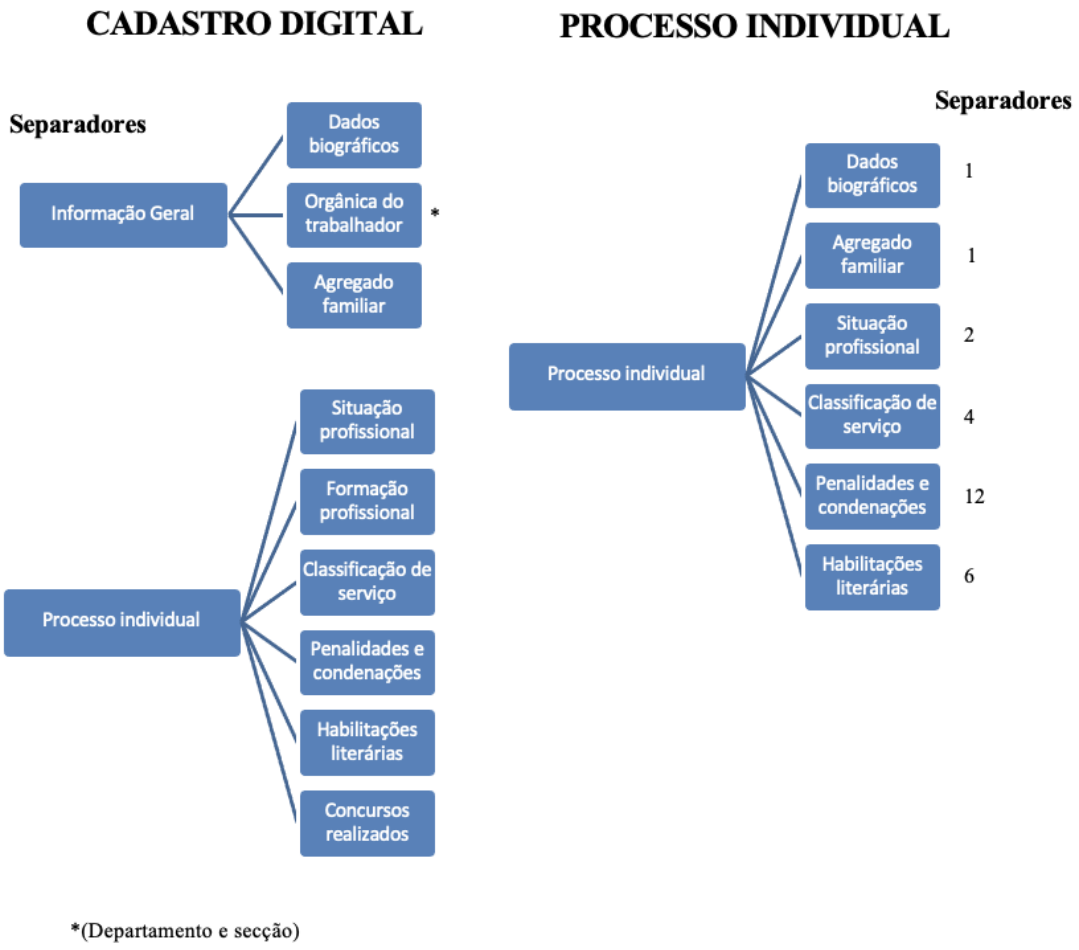
Fonte: DARH da CMVC.

ANEXO 3: Tipos de Processo do Trabalhador

TPF – Tipo de Processo de Funcionário
PFOR – Pedido de formação extraordinária
NEFO – Necessidades de formação - Plano
TRES – Processo trabalhador-estudante
ACUF – Acumulação de funções
ABOF – Abono de família
ACS – Acidentes de serviço
IS – Incidente de serviço
APOS – Processo de aposentação
JMED – Processo de junta médica
POC – Processo de candidatura IEFP
IEFP – Doença trabalhadores IEFP
PDIS – Processo disciplinar
PENH – Penhora de vencimento
PSUB – Processo pensão sobrevivência
RECL – Processo de reclamação de funcionários
RHA – Recursos Humanos - Assiduidade
RHES – Recursos Humanos – Pedidos de estágios
RHPF – Recursos Humanos – Plano de férias
RHSV – Recursos Humanos – Escalas de serviço
RH – Recursos Humanos
PRCON – Processo Concursal
MOBPC – Processo Concursal por Mobilidade
SIADAP – Processo avaliação trabalhador (SIADAP)
RHCF – Recursos Humanos - Mapas de custas fiscais
RATI – Recaída de acidentes de serviço trabalhadores IEFP
PVEX – Penhora vencimento externos
PSUB – Processo pensão sobrevivência
PINV – Pensão de Invalidez
PEXT – Pedidos ex trabalhadores
PENHNT – Penhora não trabalhadores
PCL – Processo Clínico do Trabalhador
MOBI – Mobilidade Interna funcionários
MOBE – Mobilidade entre órgãos
DPR – Processo Doenças Profissionais
ARH – Recursos Humanos (Avulso)
ATIE – Acidentes de serviço trabalhadores IEFP
ATR – Acidente de Serviço Recaída próprio ano
ACSR – Acidentes de Serviço – Recaída

Fonte: DARH da CMVC.

ANEXO 4: Cadastro Digital / Processo Individual do Trabalhador



Fonte: Elaboração própria.