



INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Da proteção de dados pessoais ao direito ao esquecimento do trabalhador à luz do RGPD

Gilana de Campos Sousa

Mestrado em Direito das Empresas e do Trabalho, especialização em Direito do Trabalho

Orientador:

Professor Doutor Mário Silveiro de Barros, Professor Auxiliar Convidado, Departamento Economia Política, Escola de Ciências Sociais e Humanas, ISCTE – Instituto Universitário de Lisboa

Co-Orientador:

Professor Doutor Iván Vizcaíno Ramos, Área de Direito do Trabalho e da Segurança Social, Faculdade de Direito da Universidade de Coruña

Outubro, 2023

Departamento de Economia Política

Da proteção de dados pessoais ao direito ao esquecimento do
trabalhador à luz do RGPD

Gilana de Campos Sousa

Mestrado em Direito das Empresas e do Trabalho, especialização em
Direito do
Trabalho

Orientador:

Professor Doutor Mário Silveiro de Barros, Professor Auxiliar
Convidado, Departamento Economia Política, Escola de Ciências
Sociais e Humanas, ISCTE – Instituto Universitário de Lisboa

Co-Orientador:

Professor Doutor Iván Vizcaíno Ramos, Área de Direito do Trabalho
e da Segurança Social, Faculdade de Direito da Universidade de
Coruña

Outubro, 2023

Dedicatória

À minha amada e estimada família, em especial, às minhas queridas mães, Ana Maria Xavier Faria de Sousa e Joaquina Xavier de Sousa, e aos meus preciosos avós maternos, Agostinho Xavier Faria de Sousa e Páscoa Justina Campos.

Agradecimentos

Ao chegar ao fim de mais uma etapa no meu percurso académico, não podia deixar agradecer a todos os que contribuíram e apoiaram para a conclusão desta fase importante da minha vida.

Começo inevitavelmente por agradecer ao meu estimado orientador, Professor Doutor Mário Silveiro de Barros, pela orientação, simpatia, disponibilidade, e todo o conhecimento jurídico que, sem pensar duas vezes, transmitiu a mim e aos meus colegas durante as aulas de processo laboral, bem como durante o período de pesquisa e elaboração da presente dissertação.

Ao meu coorientador, Professor Doutor Iván Vizcaíno Ramos, pelo apoio, e disponibilização de material, em especial no que respeitou ao direito espanhol.

A todo o corpo docente que, ao longo dos dois anos do curso de mestrado, mostrou preocupação na transmissão de conhecimento a mim, e aos meus colegas, incentivando-nos sempre a explorar o nosso senso jurídico. Um agradecimento especial aos Professores Doutores Francisco Nicolau Domingos, Luís Vasconcelos Abreu e Maria Luísa Alves.

À minha família, por acreditar, incentivar e motivar sempre a alcançar os meus sonhos e objetivos pessoais e académicos.

Aos meus colegas de curso, pelo espírito de entreajuda que conseguimos desenvolver na turma, em especial, a minha companheira desta jornada, Alexandra Nunes.

Aos meus amigos, por toda a amizade e força na elaboração deste trabalho, em especial à Jéssica Matilde Macuiane, pelas tardes de sábados e domingos passadas no caleidoscópio.

Por fim, um agradecimento muito especial a Deus, pelo suporte emocional e capacitação, por desenvolver em mim a força, dedicação, determinação, e persistência necessárias para levar o presente trabalho a bom porto.

A todos que, direta ou indiretamente contribuíram para a conclusão desta etapa, o meu infinito agradecimento.

Resumo

Num cenário onde os dados pessoais são divulgados de forma cada vez mais célere, trazendo consequências devastadoras para os titulares dos mesmos, é importante que os responsáveis pelo tratamento destes dados possam garantir ao seu titular o tratamento consciente e direcionado para o fim específico ao qual os dados foram recolhidos.

Essa exigência torna-se ainda maior num cenário de relação contratual, especialmente, numa relação laboral, onde existe um vínculo jurídico entre a entidade patronal e o trabalhador. Evidentemente que neste contexto, as exigências para o cumprimento de regras sobre a proteção de dados pessoais do trabalhador tornam-se maiores, estando a entidade patronal vinculada ao cumprimento das normas de segurança e proteção dos dados pessoais, enquanto entidade responsável pelo tratamento.

Com este enquadramento em mente, e a pensar na relação laboral, a presente dissertação, intitulada “*Da proteção de dados pessoais ao direito ao esquecimento do trabalhador à luz do RGPD*”, tem como objetivo a análise das regras de proteção de dados do trabalhador à luz do Regulamento Geral de Proteção de Dados da União Europeia, bem como à luz dos instrumentos nacionais, nomeadamente, o Código do Trabalho. De igual modo, pretende-se perceber de que forma esses instrumentos efetivamente tutelam os direitos de personalidade do trabalhador, em especial, o direito ao esquecimento e as condições do exercício deste direito por parte do trabalhador.

Desta forma, pretende-se entender de que forma as regras e legislação sobre a proteção de dados pessoais ajudaram a desenvolver o direito ao esquecimento e, consequentemente, os fundamentos para o seu exercício por parte do trabalhador.

Certos de que a relação laboral compreende diversas fases, esta análise será efetuada consoante as fases da relação, assim, importará analisar a fase pré-contratual, contratual e pós contratual da relação entre o empregador e o trabalhador e em que medida, em cada uma destas fases, o trabalhador poderá exercer o direito ao esquecimento previsto no RGPD.

Palavras-chave: Dados; Esquecimento; Responsável; Trabalhador; Empregador.

Absctrat

In a scenario where personal data is disclosed ever more quickly, with devastating consequences for the data subjects, it is important that those responsible of the treatment can guarantee that the data subject is treated with awareness and directed towards the specific purpose for which the data was collected.

This requirement becomes even greater in the context of a contractual relationship, especially an employment relationship, where there is a legal link between the employer and the employee. Clearly, in this context, the demands for compliance with rules on the protection of the employee's personal data become greater, with the employer being bound to comply with the rules on the security and protection of personal data, as the entity responsible for treatment.

With this framework in mind, and with the employment relationship in mind, this dissertation, entitled "*From the protection of personal data to the employee's right to be forgotten in the light of the GDPR*", aims to analyze the data protection rules of the employee in the light of the European Union's General Data Protection Regulation, as well as in the light of national instruments, namely the Labor Code. In the same way, the aim is to understand how these instruments effectively protect the employee's personality rights, in particular the right to be forgotten and the conditions for the employee to exercise this right.

The aim is to understand how the rules and legislation on the protection of personal data have helped to develop the right to be forgotten and, consequently, the grounds for its exercise by the employee.

Certain that the employment relationship comprises several phases, this analysis will be carried out according to the phases of the relationship, so it will be important to analyze the pre-contractual, contractual, and post-contractual phases of the relationship between the employer and the employee and to what extent, in each of these phases, the employee can exercise the right to be forgotten provided for in the GDPR.

Keywords: Data; Forgotten; Responsible; Employee; Employer.

Índice

Dedicatória	
Agradecimentos.....	i
Resumo.....	iii
Absctrat	v
Glossário de siglas e abreviaturas.....	ix
Introdução.....	1
CAPÍTULO I – CONTEXTUALIZAÇÃO E FONTES NORMATIVAS DA PROTEÇÃO DE DADOS E DO DIREITO AO ESQUECIMENTO NAS RELAÇÕES LABORAIS	3
1. Contextualização da necessidade da proteção de dados pessoais.....	3
2. Fontes normativas de direito internacional e europeu	6
2.1. Declaração Universal dos Direitos Humanos (DUDH).....	6
2.2. Pacto Internacional sobre os Direitos Cívicos e Políticos (PIDCP)	7
2.3. A Organização Internacional do Trabalho (OIT) e seu contributo	7
2.4. Carta dos Direitos Fundamentais da União Europeia (Carta).....	8
2.5. Convenção Europeia dos Direitos do Homem (CEDH).....	10
2.6. Convenção 108.º do Conselho da Europa de 1981	11
2.7. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho.....	12
2.8. O Regulamento Geral sobre a Proteção de Dados (RGPD).....	14
3. Fontes normativas de Direito nacional	16
3.1. A Constituição da República Portuguesa (CRP)	16
3.2. A Lei n.º 58/2019, de 8 de agosto - Lei de Proteção de dados	17
3.3. O Código do Trabalho (CT)	19
CAPÍTULO II – DIREITO COMPARADO	21
4. Da relevância do direito comparado.....	21
4.1. Ordenamentos jurídicos europeus	22
4.1.1. Alemanha.....	22
4.1.1.1. O contributo da Lei de Hesse	22
4.1.1.2. Lei Federal de proteção de dados, de 30 de junho de 2017	23
4.1.2. Espanha	25
4.1.2.1. Percurso para a legislação sobre a proteção de dados na Espanha	25
4.1.2.2. Lei Orgânica 3/2018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e Garantia dos Direitos Digitais, doravante, LOPDGDD.....	26
4.2. Ordenamentos jurídicos de expressão portuguesa	29
4.2.1. Cabo Verde.....	29
4.2.2. Moçambique	32

CAPÍTULO III – DA PROTEÇÃO DE DADOS PESSOAIS AO DIREITO A SER ESQUECIDO .. 35

5. Relevância da regulamentação da matéria de proteção de dados e do direito ao esquecimento	35
5.1. Definição de conceitos-chave	35
5.2. Da importância do direito da proteção de dados pessoais	36
6.Relevância do direito ao esquecimento no direito do trabalho	38
6.1. O Conceito do direito ao esquecimento	38
6.3. A natureza jurídica e o exercício efetivo do direito ao esquecimento	42
6.4. O direito ao esquecimento nas relações laborais	45
7. O contributo do processo C-131/12, Google Spain SL, Google Inc. v. Agência Espanhola de Proteção de Dados, Mario Costeja González, 13 de maio de 2014, em síntese	55
8. Os passos para o exercício do direito ao esquecimento	60
9. Conclusão	62
11. Bibliografia e Referências	65

Glossário de siglas e abreviaturas

Ac.- Acórdão;

AEPD – Agência Espanhola de Proteção de Dados;

Al. - Alínea;

Art.º - Artigo;

Carta – Carta dos Direitos Fundamentais da União Europeia;

CC – Código Civil;

CEDH – Convenção Europeia dos Direitos do Homem;

CNPD – Comissão Nacional de Proteção de Dados;

CPC – Código de Processo Civil;

CPT - Código de Processo do Trabalho;

Crf. – Conforme;

CRP – Constituição da República Portuguesa;

CT – Código do Trabalho;

Diretiva - Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995;

DL – Decreto-Lei;

DUDH – Declaração Universal dos Direitos do Homem;

EM – Estado-Membro;

LOPDGDD – Lei Orgânica 3/1018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e Garantia dos Direitos Digitais;

N.ºs – Números;

OIT – Organização Internacional do Trabalho;

OJ – Ordenamento jurídico;

ONU – Organização das Nações Unidas;

P. – Página;

PIDCP - Pacto Internacional sobre os Direitos Civis e Políticos;

PP. – Páginas;

RGPD – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados que revogou a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);

SS. - Seguintes;

STJ – Supremo Tribunal de Justiça;

TEDH – Tribunal Europeu dos Direitos do Homem;

TFUE - Tratado sobre o Funcionamento da União Europeia;

TJUE – Tribunal de Justiça da União Europeia;

UE – União Europeia;

Vol. – Volume.

Introdução

A globalização, o fenómeno migratório e a informatização de dados têm vindo a alterar o *modus operandi* quer dos responsáveis pelo tratamento dos dados pessoais, quer dos seus titulares, que têm vindo a tomar cuidados a dobrar, de modo que os seus dados não possam ser tratados para fins alheios aos que foram recolhidos.

Não está apenas em causa o tratamento propriamente dito, mas também, todas as operações que antecedem e sucedem esse tratamento, designadamente, a recolha, a conservação, a disponibilização e posteriormente, o apagamento dos mesmos.

A proteção de dados pessoais é importante não apenas no âmbito da relação de trabalho já existente, mas também, na fase anterior à celebração do contrato de trabalho, quando estamos perante candidatos a emprego, sendo que mesmo nestas situações, o responsável pelo tratamento dos dados tem obrigações inerentes à sua posição de responsável pelo tratamento dos dados dos respetivos candidatos e, igualmente, na fase posterior à cessação do contrato de trabalho, essas obrigações continuam a recair sobre o responsável pelo tratamento dos dados quando os mesmos não tenham sido apagados.

O Regulamento Geral de Proteção de Dados, Regulamento (UE) n.º 679/2016, de 27 de abril (RGPD) foi aprovado, entre outros, com o objetivo de esclarecer os princípios e regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais, por forma a que não possam ver violados quer pelos responsáveis pelo tratamento, quer por terceiros.

Adicionalmente, o considerando primeiro do RGPD reconhece que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental, sendo essa ideia corroborada pelo artigo 8.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia (Carta) e o artigo 16.º, n.º 1 do Tratado sobre o Funcionamento da União Europeia (TFUE) que estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

Desta forma, a análise da importância e contributo da proteção de dados pessoais ao direito ao esquecimento do trabalhador, bem como os mecanismos do exercício do direito ao esquecimento por parte do candidato ao emprego, trabalhador e ex-trabalhador, são objeto de estudo da presente dissertação.

CAPÍTULO I – CONTEXTUALIZAÇÃO E FONTES NORMATIVAS DA PROTEÇÃO DE DADOS E DO DIREITO AO ESQUECIMENTO NAS RELAÇÕES LABORAIS

1. Contextualização da necessidade da proteção de dados pessoais

A proteção dos dados pessoais tem vindo a ser discutida, a nível mundial, há algum tempo. No entanto, é necessário, igualmente, compreender a motivação e a necessidade dessa proteção nos dias de hoje.

Assim, e seguindo o pensamento de Jeroen Van Den Hoven¹, são quatro tipos de razões para a recolha de dados pessoais, razões essas que poderão nos ajudar a compreender a lógica para o armazenamento de dados no presente e no futuro. Em primeiro lugar, os organismos governamentais, podem querer ter o acesso aos dados dos cidadãos para os servir melhor, isto é, a fim de poder providenciar melhores serviços, estes terão de conhecer uma boa parte dos dados pessoais dos cidadãos, pelo que, poderão alertar relativamente a certos benefícios que os cidadãos não têm conhecimento de que têm direito. Pensemos, por exemplo, nos serviços de saúde. Em segundo lugar, a mesma lógica aplicar-se-á aos comerciantes e empresas, isto é, os comerciantes querem ser capazes de servir melhor aos seus clientes. Neste sentido, quanto mais informações souberem sobre estes, melhor poderão prestar os seus serviços, exemplo disso, é o facto de muitos clientes não terem problemas em receber alertas comerciais que sejam dos seus interesses e muitos, parecem estar dispostas a disponibilizar os seus dados pessoais em troca de ofertas comerciais, bónus, descontos, etc. Em terceiro lugar, os comerciantes e as empresas têm também razões estritamente prudenciais para recolher ou acumular dados pessoais, tanto dos seus clientes como dos seus parceiros de transações e dos seus trabalhadores. Geralmente, estas razões não estão relacionadas com os interesses das pessoas em causa, mas antes com a transação ou contrato que se celebra.

A relevância desta proteção também se justifica com o argumento da certeza e segurança jurídica, isto porque, muitas vezes, a outra parte pode não cumprir as suas promessas, violar o contrato ou comprar sem pagar. Nestes casos, considera-se que uma informação adequada sobre as partes envolvidas, por exemplo, informações sobre os riscos de crédito ou o desempenho comercial anterior, é extremamente útil para avaliar os riscos associados à transação. Talvez

¹ Jeeroen. Van Den Hoven (2008), em “Information technology, privacy, and the protection of personal data”, Information technology and moral philosophy, Cambridge: Cambridge University Press, (Online), pp. 304- 306. Disponível em: <https://repository.tudelft.nl/islandora/object/uuid:5f1296dc-8d5c-4224-80c6-c5af435a77cc/datastream/OBJ/download>.

ainda mais fundamental: para poder confiar nas partes; para a (re) identificação dos parceiros individuais, sendo uma condição necessária para construir uma imagem fiável do historial de interações de alguém.

Ainda no seguimento do mesmo autor, no que diz respeito às relações laborais, este explica que, a utilização da tecnologia da informação na relação entre empregador e empregado pode ser explicada em termos da teoria do agente principal, segundo a qual o principal, por exemplo, um empregador, tem sempre o problema de se certificar de que o empregado (o agente) está a fazer o que deve fazer quando está fora de vista. Por conseguinte, o empregador, muitas vezes recorre a métodos de vigilância do trabalhador, suportando o custo, por trabalhador, a associado a estes métodos. Isto explica a explosão da monitorização e vigilância do local de trabalho através de registos, câmaras, crachás inteligentes, entre outros².

Adicionalmente, o autor defende que o governo também tem razões para tentar obter informações sobre os cidadãos, razões que não se prendem primária e diretamente com os interesses individuais dos cidadãos sobre os quais as informações são recolhidas, mas sim com o interesse público. Sendo que uma das tarefas centrais do governo é a produção e manutenção de bens públicos, um dos problemas centrais será, certamente a gestão dos bens públicos e a gestão do acesso aos bens públicos e, mais concretamente, o problema da exclusão dos cidadãos dos bens públicos, por essa razão, aqui também será relevante e do interesse público o tratamento de certos dados pessoais.

O autor conclui que existem quatro razões morais que justificam a proteção dos dados pessoais. Em primeiro lugar está a preocupação com os danos que podem ser causados com a utilização indevida dos dados recolhidos, principalmente por terceiros, podendo essa utilização ser prejudicial ao titular dos dados. Em segundo lugar está a prevenção da exploração dos dados pessoais nos mercados, relacionado com o uso abusivo da informação disponibilizada pelo titular dos dados. Em terceiro lugar, a prevenção da desigualdade e da discriminação, muito pensada para as situações em que os titulares de dados não têm o controlo da utilização a que os seus dados estão a ser alvo, e se de facto são tratados seguindo as normas orientadoras da licitude do tratamento. Por fim, a quarta razão está relacionada com a liberdade e autonomia da vontade, na medida em que é através da liberdade pessoal que o titular dos dados poderá decidir o que fazer ou não com os seus dados, liberdade essa que é restringida quando a

² Jeeroen. Van Den Hoven (2008), em “Information technology, privacy, and the protection of personal data”, ob. cit., p. 305.

responsabilidade pelo tratamento desses dados é transferida para um terceiro, assim os titulares terão a sua liberdade limitada³.

³ Jeeroen. Van Den Hoven (2008), em “Information technology, privacy, and the protection of personal data”, ob. cit., p. 319.

2. Fontes normativas de direito internacional e europeu

2.1. Declaração Universal dos Direitos Humanos (DUDH)

A proteção dos dados pessoais surge com o impulso da evolução da tecnologia de informação aliado ao paradigma internacional nos planos social, comercial, laboral, e de relações privadas. Situações essas que geraram e continuam a gerar enormes obstáculos em questões relacionadas com a proteção dos dados que são recolhidos e tratados, criando uma maior consciencialização para quem tenha o acesso a tais informações. Desta forma, e por conta dessa consciencialização, a matéria da proteção de dados pessoais ganhou tanta relevância que rapidamente se verificou a necessidade de criação de legislação específica para a temática.

A DUDH foi adotada e proclamada pela Assembleia Geral das Nações Unidas, em Paris, por meio da resolução 217 A III em 10 de dezembro de 1948. Assim, já desde essa altura se previa uma especial proteção relativamente a privacidade. Desta forma, apesar de se tratar de uma temática relativamente recente, que passou a ser discutida e efetivada com maior pertinência com o surgimento do RGPD, a sua relevância já é de tempos passados, uma vez que com a DUDH de 1948, já se reconhecia o direito à privacidade, estando expressamente previsto que, *“Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei⁴.”*

Além do mais, o artigo 8.º da DUDH, estabelece a proteção legal e o recurso jurisdicional para os cidadãos que sofram violações nos seus direitos fundamentais, entre os quais e inevitavelmente, as violações que respeitassem o direito à privacidade, desta forma, dispõe o preceito legal que, *“Toda a pessoa tem direito a recurso efetivo para as jurisdições nacionais competentes contra os actos que violem os direitos fundamentais reconhecidos pela Constituição ou pela lei⁵.”*

Ora, podemos concluir que o facto de a DUDH já prever a proteção da vida privada e familiar através do direito à privacidade, serviu de base e inspiração para a posterior legislação na matéria. Razão pela qual acreditamos que os diplomas posteriores vieram inovar, atualizar e concretizar as regras específicas da proteção de dados pessoais.

⁴ Artigo 12.º da Declaração Universal dos Direitos do Humanos.

⁵ Artigo 8.º da Declaração Universal dos Direitos Humanos.

2.2. Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP)

O pacto internacional sobre os direitos civis e políticos, é um instrumento multilateral de direitos humanos que foi adaptado e aberto à assinatura, ratificação e adesão pela resolução 2200-A (XXI) da Assembleia das Nações Unidas, em 16 de dezembro de 1966, tendo o seu início de vigência na ordem internacional em 23 de março de 1976. Foi assinado por Portugal em 7 de outubro de 1976, tendo entrado em vigor na ordem jurídica portuguesa apenas em 15 de setembro de 1978. Este instrumento tem como premissa, estampada no seu preâmbulo, o reconhecimento de que, de acordo com a DUDH, não se pode realizar o ideal do ser humano livre, gozando das liberdades civis e políticas, libertos do terror e da miséria, a menos que se criem condições que permitam a cada pessoa gozar dos seus direitos civis e políticos, assim como dos seus direitos económicos, sociais e culturais.

Desta forma, no que a matéria de proteção de dados diz respeito, o artigo 17.º do PIDCP estabelece que *“Ninguém será objeto de intervenções arbitrarias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação”*, e acrescenta que *“Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados”*⁶.

Sendo essa proteção garantida pelo artigo 14.º que estabelece a garantia do acesso aos tribunais e à justiça nos casos em que o cidadão vê os seus direitos, liberdades e garantias violados.

2.3. A Organização Internacional do Trabalho (OIT) e seu contributo

Relativamente a esta matéria, a OIT adotou em 1997 o repertório de recomendações práticas sobre a proteção de dados pessoais⁷. Pese embora tratar-se apenas de recomendações, ou seja, sem carácter vinculativo, uma vez que a OIT é a organização mundialmente responsável pela formulação e aplicação das normas internacionais do trabalho, acreditamos que essas recomendações terão tido certamente relevância na construção das normas de proteção de dados pessoais.

⁶ Artigo 17.º do Pacto Internacional sobre os Direitos Civis e Políticos

⁷*Protection of workers personal data*, disponível em: https://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf.

Desta forma, foram aprovadas diretrizes para a regulação sobre ficheiros informatizados de dados de carácter pessoal, que consistem em procedimentos a adotar para a regulação dos ficheiros informatizados de dados de carácter pessoais que serão definidos por cada Estado, sem prejuízo das orientações estabelecidas, nomeadamente, no que diz respeito aos princípios relativos às garantias mínimas que devem ser consagradas na legislação nacional, a saber: o princípio da legalidade equidade, princípio da exatidão, princípio da finalidade especificada, princípio da pessoa interessada, princípio da não discriminação, e princípio da segurança.

Para o presente estudo, importa refletir sobre as recomendações referentes aos princípios gerais sobre o tratamento dos dados pessoais dos trabalhadores, previstas no ponto 5, que prevê que os dados pessoais do trabalhador devem ser objeto de um tratamento legal e lícito, e apenas para razões relevantes para o trabalho a desenvolver pelo trabalhador, e em princípio devem apenas ser utilizados para a finalidade para a qual foram inicialmente recolhidos.

De igual forma, o ponto 11, é relevante, na medida em que prevê a possibilidade de o trabalhador poder exigir que os dados pessoais incorretos ou incompletos, bem como os dados que sejam objeto de um tratamento ilícito ou incompatível com a finalidade para a qual foram recolhidos, possam ser suprimidos ou retificados. Por seu turno, se o empregador se recusar a retificar dos dados pessoais do trabalhador, este tem o direito de incluir ou acrescentar ao seu processo uma nota com os motivos do seu desacordo com o tratamento dos dados não retificados, sendo que qualquer utilização dos dados posterior deverá indicar que esses dados foram objeto de contestação por parte do trabalhador, e deverá ser anexada a referida nota.

Adicionalmente, também está previsto que qualquer lei, regulamento ou convenção coletiva de trabalho, diretiva laboral ou política desenvolvida em conformidade com as disposições dessas recomendações deve prever um procedimento para que os trabalhadores possam contestar o cumprimento das normas relativas ao tratamento dos seus dados pessoais pela entidade empregadora. Assim sendo, deverão ser estabelecidos procedimentos para receber e tratar das queixas dos trabalhadores, sendo que estes procedimentos devem ser simples e facilmente acessíveis aos trabalhadores.

2.4. Carta dos Direitos Fundamentais da União Europeia (Carta)

A Carta dos direitos fundamentais da União Europeia, foi proclamada em 7 de dezembro de 2000. No entanto, sem qualquer efeito jurídico vinculativo, constituindo apenas um compromisso político. Assim, seriam necessárias adaptações para que Carta adquirisse o mesmo valor dos Tratados, facto que levou, sete anos depois, a uma segunda proclamação da

Carta em 12 de dezembro de 2007. Por conseguinte, o cumprimento da Carta passou a ser obrigatório para as instituições da união, órgãos e agências e para os Estados-Membros quando aplicam o direito da União Europeia, com a entrada em vigor do Tratado de Lisboa a 1 de dezembro de 2009⁸.

Desta forma, a Carta surge pela necessidade de reunir num texto único e reafirmar o conjunto de direitos dos cidadãos europeus, direitos civis, políticos, económicos e sociais, que se encontravam dispersos por diversos instrumentos legislativos, nomeadamente, na DUDH, na Carta Social Europeia, na Carta Comunitária dos Direitos Sociais Fundamentais dos Trabalhadores, bem como nos tratados europeus, e na jurisprudência da UE. E ainda, com o objetivo de conferir-lhes visibilidade e, ao mesmo tempo, assegurar que as instituições da união europeia e os Estados Membros sempre que aplicam a legislação da união respeitem os direitos consagrados na Carta, e reforça a questão da proteção dos cidadãos⁹.

Sendo um diploma relativamente recente, a Carta reflete nos seus artigos, preceitos relacionados com a proteção de dados pessoais e vida privada, conforme artigos 7.º e 8.º. Assim, o artigo 7.º da Carta, dispõe o respeito pela vida privada e familiar, prevendo que *“Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações”*¹⁰.

Por seu turno, o artigo 8.º da Carta com epígrafe “Proteção de dados pessoais”, estabelece nos seus diversos números da tutela dos dados pessoais, dispondo que *“Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito”*, acrescentado que *“Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com fundamento legítimo previsto por lei. Todas as pessoas têm direito de aceder aos dados coligidos e que lhes digam respeito e de obter a respetiva retificação”* e concluindo que *“O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”*¹¹.

Nestes termos, vislumbra-se que a Carta pode ser entendida como uma norma que surgiu motivada pelo avanço tecnológico associado aos novos métodos de recolha e armazenamento de dados, que tem como consequências, ameaças à intimidade privada, ao direito à privacidade,

⁸ Cfr. Preâmbulo e disposições gerais sobre a interpretação e aplicação da Carta, em especial o artigo 51.º.

⁹ Cfr. Preâmbulo da Carta dos Direitos Fundamentais da União Europeia.

¹⁰ Artigo 7.º da Carta dos Direitos Fundamentais da União Europeia.

¹¹ Artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

entre outros. Direitos estes que são especialmente vulneráveis e suscetíveis de serem lesados com o uso das novas tecnologias¹².

2.5. Convenção Europeia dos Direitos do Homem (CEDH)

A Convenção Europeia dos Direitos do Homem (CEDH), é um tratado internacional celebrado pelos Estados Membros do Conselho da Europa, adotada em Roma em 4 de novembro de 1950, tendo entrado em vigor na ordem internacional no dia 3 de setembro de 1953. Em Portugal, a CEDH foi assinada em 22 de setembro de 1976, com entrada em vigor a 9 de novembro de 1978¹³.

Inspirada pela DUDH, a CEDH reflete, assim, a manifestação da necessidade de legislar um conjunto de direitos humanos para os cidadãos europeus, sendo, por isso, o primeiro instrumento com carácter legalmente vinculativo após a proclamação da DUDH¹⁴.

Com objetivo de tomar as primeiras providencias apropriadas para assegurar a garantia coletiva de certo número de direitos enunciados na DUDH, através da CEDH, foi convencionado, entre outros, o disposto no artigo 8.º, referente aos respeito pela vida privada e familiar, dispondo no n.º 1 que *“Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”* e no n.º 2, estabelecendo o seguinte *“Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providencia que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.”*¹⁵.

Assim, embora a CEDH tenha nascido com o intuito de incorporar e tornar vinculativos os direitos consagrados na DUDH, a CEDH distingue-se da DUDH pela criação de normas vinculativas e pela introdução de um mecanismo judiciário reacionário que permitisse o controlo da aplicação da legislação em vigor, esta é a primeira Convenção de Direitos Humanos

¹² Suárez, Arturo Montesdeoca (2022), Tese de Doutoramento, *De la protección de datos personales a la construcción de un catálogo de derechos digitales de las personas trabajadoras*, Universidade de Las Palmas de Gran Canaria, outubro de 2022, p. 81, disponível em <https://accedacris.ulpgc.es/handle/10553/119852>.

¹³ Crf. Lei n.º 65/78, de 13 de outubro, aprova para ratificação, a Convenção Europeia dos Direitos do Homem.

¹⁴ Cfr. Direção geral da Educação, Convenção Europeia dos Direitos Humanos – 1950-2020, disponível em <https://cidadania.dge.mec.pt/sites/default/files/pdfs/convencao-europeia-dos-direitos-humanos-1950-2020.pdf>.

¹⁵ Artigo 8.º, n.º 1 da Convenção Europeia dos Direitos do Homem.

a estabelecer um tribunal internacional independente – o Tribunal Europeu dos Direitos Humanos¹⁶. Esgotadas as vias judiciais internas, os cidadãos dos Estados vinculados à Convenção, podem agora recorrer a este Tribunal, criado especialmente para julgar e punir as violações dos direitos consagrados pela Convenção¹⁷.

2.6. Convenção 108.º do Conselho da Europa de 1981

A Convenção para a Proteção das Pessoas relativamente ao Tratamento automatizado de Dados de Carácter Pessoal, foi assinada em 28 de janeiro de 1981, em Estrasburgo, teve o seu início de vigência na ordem internacional a 01 de janeiro de 1985, e início de vigência em Portugal, apenas em 01 de janeiro de 1994¹⁸. Tem como finalidade a proteção de todas as pessoas, independentemente da sua nacionalidade ou residência, no que diz respeito ao tratamento dos seus dados pessoais, contribuindo assim para o respeito dos seus direitos humanos e liberdades fundamentais e, em especial, do direito à vida privada, face ao tratamento automatizado dos seus dados de carácter pessoal que lhes digam respeito (proteção dos dados)¹⁹.

Desta forma, o capítulo II da referida Convenção, diz respeito aos princípios para a proteção de dados, ou seja, a qualidade dos dados, as categorias especiais de dados, a segurança dos dados, as garantias adicionais para o titular dos dados, as exceções e restrições e a proteção mais ampla. Importa, por isso, destacar alguns artigos que têm importância nesta matéria.

O artigo 5.º relativo à legitimidade do tratamento de dados e da qualidade dos mesmos, assim, nos termos do n.º 1 deste artigo, o tratamento de dados deverá ser proporcional à finalidade legítima prosseguida e refletir em todas as fases do tratamento, um justo equilíbrio entre todos os interesses envolvidos, públicos ou privados, e dos direitos e liberdades em causa.

O artigo 6.º diz respeito às categorias especiais de dados, e estabelece que “*Os dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas*

¹⁶ Artigo 19.º da CEDH - *A fim de assegurar o respeito dos compromissos que resultam, para as Altas Partes Contratantes, da presente Convenção e dos seus protocolos, é criado um Tribunal Europeu dos Direitos do Homem, a seguir designado “o Tribunal”, o qual funcionará a título permanente.*

¹⁷E-book: Declaração Universal dos Direitos Humanos | Convenção Europeia dos Direitos Humanos. Anotações pelos estudantes da Faculdade de Direito da Universidade do Porto. Coordenação: Anabela Costa Leão, Inês Neves, Juliana Ferraz Coutinho, Luísa Neto. Edição Universidade do Porto. Reitoria. 2019, p. 203, disponível https://sigarra.up.pt/fdup/pt/web_gessi_docs.download_file?p_name=F-1209942143/ebook_DH.pdf

¹⁸ Cfr. Aprovada pela Resolução da Assembleia da República n.º 23/93, de 9 de julho, retificada pela Retificação n.º 10/93, de 20 de agosto e retificada pelo Decreto do Presidente da República n.º 21/93, de 9 de julho.

¹⁹ Artigo 1.º da Convenção 108.º do Conselho da Europa de 1981.

ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objeto de tratamento automatizado desde que o direito interno preveja as garantias adequadas. O mesmo será aplicável para os dados de carácter pessoal relativos a condenações penais.”²⁰.

Relativamente à segurança dos dados, dispõe o artigo 7.º que “*Para a proteção dos dados de carácter pessoal registados em ficheiros automatizados devem ser tomadas medidas de segurança apropriadas contra a destruição, acidental ou não autorizada, e a perda acidental e também contra o acesso, modificação ou difusão não autorizados.*”²¹.

Quanto à proteção, o artigo 10.º estabelece que “*As Partes comprometem-se a estabelecer sanções de via de recurso apropriadas em face da violação das disposições do direito interno que confiram eficácia aos princípios básicos para a proteção dos dados, enunciados no presente capítulo.*”²².

A Convenção, estabelece ainda que, cada Parte, compromete-se a aplicar as suas disposições nesta matéria, em especial, relativamente ao tratamento de dados sob a sua jurisdição nos setores público e privado, garantindo assim o direito de todas as pessoas à proteção dos seus dados pessoais²³.

2.7.A Diretiva 95/46/CE do Parlamento Europeu e do Conselho

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi um marco para a regulação comunitária nesta matéria de proteção de dados pessoais propriamente dita.

A Diretiva tinha como objeto, conforme o artigo 1.º, o asseguramento da proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente, do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, bem como a não proibição ou restrição da livre circulação de dados pessoais entre Estados Membros por razões relativas à proteção assegurada.

²⁰ Crf. Artigo 6.º da Convenção 108.º do Conselho da Europa de 1981.

²¹ Crf. Artigo 7.º da Convenção 108.º do Conselho da Europa de 1981.

²² Crf. Artigo 10.º da Convenção 108.º do Conselho da Europa de 1981.

²³ Cfr. Artigo 3.º, n.º1 da Convenção 108.º do Conselho da Europa de 1981.

Nos termos da Diretiva, entendia-se por dados pessoais, qualquer informação relativa a uma pessoa singular identificada ou identificável (“pessoa em causa”), sendo que é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente, por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

A Diretiva, aplicava-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro²⁴ ou a ele destinados.

Desta forma, e numa perspetiva mais abrangente, podemos concluir que, esta Diretiva pretendia ampliar o escopo de proteção dos dados pessoais do titular dos dados, já refletido na Convenção 108.º do Conselho da Europa de 1981²⁵, exemplo disso é o considerando 11 da Diretiva, que previa “*Considerando que os princípios da proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, contidos na presente Diretiva, precisam e ampliam os princípios contidos na Convenção do Conselho da Europa, de 28 de Janeiro de 1981, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais.*”²⁶.

Quanto ao direito ao esquecimento, a Diretiva já dava pistas ao que viria a ser hoje o conhecido direito a ser esquecido. Apesar de não estar previsto na Diretiva nenhuma norma expressa relativamente a este direito, o mesmo poderia ser alcançado com o recurso a dois outros direitos, direito ao acesso e direito de oposição da pessoa em causa, conforme os artigos 12.º e 14.º respetivamente, como se demonstrará mais adiante no presente trabalho, com o estudo do Processo C-131/12, Google Spain SL e Google Inc. contra a Agência Espanhola de Proteção de Dados e Mario Costeja González.

Assim, nos termos do artigo 12.º, al. b) da Diretiva, os Estados-Membros tinham de garantir às pessoas em causa o direito de obterem do responsável pelo tratamento, consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpria com o disposto na Diretiva, nomeadamente, devido ao carácter incompleto ou inexato desses dados. E nos

²⁴ *Qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico*, artigo 2.º, al. c) da Diretiva 95/46/CE.

²⁵ Suárez. Arturo Montesdeoca, De la protección de datos personales a la construcción de un catálogo de derechos digitales de las personas trabajadoras, ob.cit., p. 83.

²⁶ A Diretiva 95/46/CE do Parlamento Europeu e do Conselho .

termos do artigo 14.º, al. a), os Estados-Membros reconheceriam à pessoa em causa o direito de, por um lado, pelo menos nos casos referidos nas alíneas e) e f) do artigo 7.º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efetuado pelo responsável pelo tratamento deixaria de poder incidir sobre esses dados. Por outro, se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de marketing direto; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros, para fins de marketing direto ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, as tais comunicações ou utilizações.

Mais de vinte anos volvidos, com o impulso da evolução tecnologia, a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados através da Diretiva mostrou-se insuficiente, havendo desta forma necessidade de atualização e de reforço da proteção jurídica atribuída pela Diretiva, razão pela qual foi aprovado o Regulamento Geral de Proteção de Dados.

2.8. O Regulamento Geral sobre a Proteção de Dados (RGPD)

O Regulamento Geral sobre a Proteção de Dados, aprovado através do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), em Bruxelas, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogou a Diretiva 95/46/CE, entrou em vigor apenas em 25 de maio de 2018. Por conseguinte, o RGPD foi aprovado com o objetivo de contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica para o progresso económico e social, para a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares²⁷.

Nos termos do artigo 288.º do TFUE, sendo um regulamento, este diploma é vinculativo, tendo um carácter geral, obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros. Ou seja, não existe a necessidade de transposição para o direito interno. O

²⁷ Considerando (2) do RGPD.

que nos leva a crer que, à partida, este diploma assegurará uma maior segurança jurídica para os titulares dos dados pessoais.

O RGPD começa por relembrar que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental, sendo que para isso, recorda que o artigo 8.º, n.º 1 da Carta e o artigo 16.º, n.º1 do TFUE estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

No elenco dos considerandos, é importante destacar o considerando n.º 4, que refere desde logo que o direito à proteção de dados pessoais não é absoluto, e deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

Pela primeira vez, e através do RGPD, é consagrado de forma expressa o direito ao apagamento dos dados, também conhecido como o direito ao esquecimento, previsto no artigo 17.º. Com a epígrafe “Direito ao apagamento dos dados (“direito a ser esquecido”)), o artigo 17.º do RGPD concede ao titular dos dados o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, colocando neste, a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos motivos elencados na norma, entre eles, na alínea a), quando os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

O tema da aplicabilidade da norma referente ao direito ao esquecimento no âmbito das relações laborais ainda não foi desenvolvido de forma detalhada. Porém, poderá entender-se que esta norma será aplicável nas relações laborais, nas suas várias fases, em especial, na medida em que, por força da cessação de um contrato de trabalho, independentemente da parte que fizer cessar o vínculo laboral, o trabalhador (titular dos dados), terá, à partida, o direito de obter do responsável pelo tratamento (entidade empregadora), o apagamento dos seus dados pessoais sem demora injustificada, desde que preenchidos determinados requisitos. Há que relembrar, porém, que este direito não é absoluto, tal como consagrado no considerando 4 do RGPD, e no seu exercício, deve de ser considerado em relação à sua função na sociedade e equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. Tema a desenvolver mais adiante no presente trabalho.

3. Fontes normativas de Direito nacional

3.1.A Constituição da República Portuguesa (CRP)

A ordem jurídica portuguesa foi pioneira, a nível mundial, no reconhecimento do direito da proteção de dados pessoais como direito fundamental²⁸. Assim, o direito à proteção de dados pessoais é uma consagração constitucional no ordenamento jurídico português. Este direito vem consagrado na CRP desde 1976, sendo que este facto assumiu uma inegável relevância jurídica em diversos aspetos, designadamente, em questões de dignidade da pessoa humana e de respeito a vida privada dos cidadãos.

Assim, o artigo 35.º da CRP, com a epígrafe “utilização da informação”, estabelece no seu n.º 1 que “todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de reconhecer a finalidade a que se destinam, nos termos da lei”. A CRP deixa ao critério da lei o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção designadamente através de entidade administrativa independente.

Nos termos do n.º 3 do mesmo artigo, “a informática não pode ser utilizada para o tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis”, ou seja, os dados enquadrados nas categorias especiais de dados pessoais, nos termos do artigo 9.º do RGPD.

O n.º 7 acrescenta que a proteção conferida aos dados informatizados, estende-se aos dados pessoais constantes de ficheiros manuais, gozando, assim, de proteção idêntica.

Ora, a consagração nacional do direito à proteção de dados pessoais constitui uma garantia deste direito, incumbindo, desde logo, à entidade responsável pelo tratamento dos dados em causa, o dever de proteção e salvaguarda dos mesmos, por forma a garantir a sua verdadeira efetivação a nível nacional.

²⁸ Cfr. <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/historico-da-cnpd/>

3.2.A Lei n.º 58/2019, de 8 de agosto - Lei de Proteção de dados

O histórico da legislação interna sobre a proteção de dados, começou pela Lei 10/91, de 29 de abril, Lei da Proteção de Dados Pessoais Face à Informática, posteriormente, foi aprovada a Lei n.º 28/94, de 29 de agosto, que aprovou medidas de reforço da proteção de dados pessoais, no seguimento do compromisso assumido com a ratificação da Convenção 108.º do Conselho da Europa de 1981.

Quatro anos depois, foi aprovada a Lei n.º 67/98, de 26 de outubro, Lei da Proteção de Dados Pessoais, foi a lei que transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, tendo aquela lei sido revogada, de forma expressa, pela Lei n.º 58/2019, de 8 de agosto, atual lei de proteção de dados portuguesa, constituindo, deste modo, a lei de execução do RGPD.

Assim, a Lei n.º 58/2019, de 8 de agosto (Lei de Proteção de Dados), é o diploma que assegura a execução, na ordem jurídica nacional, do atual Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD), sendo esse o objeto da lei.

Quanto ao âmbito de aplicação, esta aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, com as exclusões contidas no 2.º do RGPD.

A Lei n.º 58/2019, estabelece, no seu artigo 28.º, regras relativas ao tratamento de dados efetuado nas relações laborais. Assim, nos termos do n.º1 deste artigo, o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no CT e respetiva legislação complementar ou noutros regimes setoriais, com as especificações previstas nesse artigo. O n.º 2 acrescenta o referido no n.º 1 abrange, igualmente, o tratamento efetuado por subcontratante ou contabilista certificado em nome do empregador, para fins de gestão de relações laborais, desde que realizado ao abrigo de um contrato de prestação de serviços e sujeito a iguais garantias de sigilo, garantido assim, ao trabalhador, igual proteção e segurança jurídica ao tratamento efetuado pelo empregador.

Por seu turno, o n.º 3 do mesmo artigo dispensa o consentimento do trabalhador como requisito de legitimidade do tratamento dos seus dados pessoais se, desse tratamento resultar uma vantagem jurídica ou económica para o trabalhador ou se o tratamento estiver abrangido pelo disposto na al. b) do n.º 1 do artigo 6.º do RGPD, referente ao tratamento no âmbito da execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados, ou seja, ao abrigo de um contrato de trabalho, ou no âmbito de um recrutamento, regra geral.

Quanto à gravação de imagens e outros dados pessoais registados através da utilização de sistemas de vídeo e outros meios tecnológicos de vigilância à distância, nos termos do artigo 20.º do CT, o n.º 4 estabelece que apenas podem ser utilizados no âmbito do processo penal, ou seja, o empregador, fora destes casos, não poderá utilizar os dados pessoais do trabalhador recolhidos por estes meios, sem prejuízo do estabelecido no n.º 5, que prevê a utilização destes dados para efeitos do apuramento de responsabilidade disciplinar do trabalhador, na medida em que o sejam, novamente, no âmbito do processo penal.

Por fim, quanto ao tratamento de dados biométricos do trabalhador, nos termos do n.º 5, este apenas é considerado legítimo para o controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados.

Quanto ao direito ao esquecimento, a Lei n.º 59/2019, estabelece, no artigo 25.º, n.º4, que o direito ao apagamento de dados pessoais publicados em jornal oficial tem natureza excecional e só se pode concretizar nas condições previstas no artigo 17.º do RGPD, nos casos em que essa seja a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença. Não prevê, assim, uma norma específica para o direito ao esquecimento no âmbito das relações laborais, aplicando-se, de igual forma, o artigo 17.º do RGPD. Por fim, nos termos do artigo 37.º, n.º 1, al. i), constitui contraordenação muito grave, não permitir, não assegurar ou dificultar o exercício dos direitos previstos nos artigos 15.º a 22 do RGPD, incluído neste intervalo, o direito ao esquecimento.

3.3.O Código do Trabalho (CT)

Sendo o Código do Trabalho o diploma master em matéria da relação laboral, dos direitos e deveres dos trabalhadores, dos empregadores, e de outros sujeitos que fazem parte desta relação, é fundamental que este diploma acompanhe o desenvolvimento tecnológico, bem como o desenvolvimento legislativo nessa matéria. Por essa razão, o CT já contempla algumas normas referentes à proteção de dados pessoais, nos artigos 14.º e seguintes, quando se refere aos direitos de personalidade.

Posto isto, o artigo 17.º do CT regula a proteção de dados pessoais, estabelecendo no seu n.º 1 que, o empregador não pode exigir do candidato ao emprego ou do trabalhador que preste informações relativas: a) à sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar a respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação; b) à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação.

O n.º 2 acrescenta que as informações previstas na alínea b) serão prestadas por médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a atividade.

Adicionalmente, o n.º 3 estabelece que o candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respetivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua retificação e atualização.

O n.º 4, por sua vez, prevê que os ficheiros e acessos informáticos utilizados pelo empregador para o tratamento de dados pessoais do candidato a emprego ou trabalhador, ficam sujeitos a legislação em vigor relativa à proteção de dados pessoais. Ou seja, a lei laboral remete-nos para a legislação em vigor relativa à proteção de dados. Legislação essa já anteriormente analisada, em especial, o RGPD e a Lei n.º 58/2019.

Desta forma, se quisermos aplicar regras relativas ao direito ao esquecimento do trabalhador, ou se quisermos aplicar o direito ao esquecimento nas relações laborais, temos de recorrer a estas normas, mais concretamente ao artigo 17.º do RGPD.

CAPÍTULO II – DIREITO COMPARADO

4. Da relevância do direito comparado

O direito comparado é uma disciplina que tem por objeto a comparação de direitos, ou seja, o estudo comparativo sistemático de diferentes ordens jurídicas com vista a identificar as semelhanças e as diferenças existentes entre elas.

Para além disso, o direito comparado contribui significativamente para o desenvolvimento do direito no plano interno. Desta forma, o conhecimento de direitos estrangeiros que é proporcionado pelo estudo de direito comparado pode revelar-se útil para a interpretação e aplicação de normas de direito nacional²⁹, bem como para interpretação e aplicação de normas de direito estrangeiro à resolução de litígios perante tribunais nacionais, por exemplo, em questões jurídicas plurilocalizadas, familiares, laborais e contratuais no geral.

Com este enquadramento em mente, no presente capítulo de estudo comparativo serão analisados diferentes ordenamentos jurídicos europeus de modo a encontrar as semelhanças e diferenças na legislação dos mesmos, no que concerne à matéria de proteção de dados pessoais, em especial, no que diz respeito ao direito ao esquecimento aplicado à figura do trabalhador. Assim, ainda que no geral as normas da união europeia sejam semelhantes, existirão algumas especificidades em cada OJ que serão relevantes e merecem apreciação. Esta análise poderá contribuir para o desenvolvimento de temas ainda não pensados no ordenamento jurídico nacional.

Por conseguinte, no âmbito da união europeia, os ordenamentos jurídicos a analisar serão o alemão, e o espanhol, devido a sua aproximação geográfica e histórica com o OJ nacional, por um lado e, por outro, por serem OJ que, a nosso ver, contribuíram e continuam a contribuir para o avanço legislativo nesta matéria.

Para além dos ordenamentos jurídicos europeus, será de igual modo importante analisar outros ordenamentos jurídicos que, embora se distanciem geograficamente do ordenamento jurídico nacional, são bastante relevantes pelo contexto histórico e pela proximidade linguística. Desse modo, a nível dos países de expressão portuguesa, serão analisados os ordenamentos jurídicos cabo-verdiano moçambicano.

²⁹ Jerónimo, Patrícia (2015), Lições de Direito Comparado, p. 16.

4.1. Ordenamentos jurídicos europeus

4.1.1. Alemanha

4.1.1.1.O contributo da Lei de Hesse

A primeira legislação sobre proteção de dados na Alemanha entrou em vigor 13 de outubro de 1970, legislação essa que ficou conhecida como *Hessisches Datenschutzgesetz* ou Lei de Hesse. Desta forma, o Estado de Hesse, na região central da Alemanha tornou-se o primeiro a introduzir uma legislação sobre a proteção de dados pessoais no âmbito local³⁰.

A Lei de Hesse tem por objeto a regulação e processamento de dados pessoais por organismos públicos no estado, bem como nos municípios e distritos. Desde a sua aprovação, esta lei tem passado por diversas revisões, tendo sido a última em 3 de maio de 2018, e última alteração em 15 de novembro de 2021, com vista a adaptar a Lei ao RGPD e a implementar a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados³¹.

Será importante fazer uma pequena análise legislativa desta lei, por forma também a perceber o impacto que a mesma teve no desenvolvimento da legislação posterior, nomeadamente, da Lei Federal Alemã. Na sua génese, a Lei de Hesse era uma lei bastante simples, contemplado apenas um total de 13 artigos. Por conseguinte, quanto ao âmbito de aplicação, o artigo 1.º da mesma especificou claramente o foco no tratamento automatizado efetuado pela própria administração pública alemã, bem como pelas empresas e instituições sujeitas a supervisão estatal. Por outro lado, no que respeita a matéria de proteção de dados propriamente dita, nos números 1 e 2 do artigo 4.º, a lei estabelece a possibilidade de o titular dos dados exercer os direitos de acesso, limitação, retificação e oposição³².

³⁰ Cfr. <http://dadospessoais.lavits.org/historico-pelo-mundo/>

³¹Cfr. Artigo 1.º da Lei de Hesse.

³²Seguimos de perto Suárez. Arturo Montesdeoca, De la protección de datos personales a la construcción de un catálogo de derechos digitales de las personas trabajadoras, ob.cit., p. 126.

No entanto, com as alterações introduzidas de modo a adaptar à lei ao RGPD, o escopo de direitos do titular dos dados foi alargado, especialmente com a previsão do direito ao apagamento (Direito ao Esquecimento)³³.

4.1.1.2. Lei Federal de proteção de dados, de 30 de junho de 2017

Posteriormente, e fruto do impulso legislativo levado a cabo pela Lei de Hesse, foi aprovada a Lei Federal Alemã, de 27 de janeiro de 1977, comumente conhecida como *Bundesdatenschutzgesetz*. Em consequência do RGPD, esta lei foi adaptada através da Lei Federal de proteção de dados, *Federal Data Protection Act (BDSG)* de 30 de junho de 2017. Desta forma, nível nacional, o Ministério Federal das relações Externas e as representações diplomáticas e consulares alemãs e instituições públicas e privadas tratam dos dados pessoais em conformidade com o Regulamento Geral sobre a Proteção de Dados e a Lei Federal de proteção de dados, *Federal Data Protection Act (BDSG)* de 30 de junho de 2017, bem como eventuais regulamentos específicos³⁴.

Esta lei autoriza as entidades públicas a efetuarem o tratamento dados pessoais se tal tratamento for necessário para o exercício da função lhes que incumbe ou se for necessário para o controlo da atividade que tenha sido conferida ao responsável pelo tratamento. No que diz respeito às entidades privadas, a lei aplica-se ao tratamento de dados pessoais total ou parcialmente automatizados e ao tratamento não automatizado de dados pessoais que façam parte de um ficheiro ou que se destinem a fazer parte de um ficheiro, exceto se o tratamento for efetuado no âmbito de uma atividade exclusivamente pessoal ou doméstica.

Adicionalmente, estão elencados diversos direitos do titular dos dados, e obrigações do responsável pelo tratamento, nomeadamente, direitos e obrigações referente às informações a fornecer quando os dados pessoais são recolhidos, direito ao acesso dos dados fornecidos e direito ao apagamento. No entanto, está excluído o direito ao apagamento quando se trate de tratamento de dados não automatizado.

Assim, nas situações em que o apagamento não for impossível ou envolver um esforço desproporcional devido ao modo específico de armazenamento e se o interesse do titular dos dados puder ser considerado mínimo, o titular não terá o direito ao apagamento e o responsável pelo apagamento não estará obrigado a apagar os dados nos termos do previsto no art.º17.º do

³³ Secção 2, ponto 34 da Lei de Hesse.

³⁴ <https://lissabon.diplo.de/pt-pt/botschaft/datenschutz>

RGPD, salvo devidas exceções previstas no mesmo artigo. Alternativamente ao apagamento, será aplicada a limitação do tratamento tal como previsto no artigo 18.º do RGPD. Porém, nenhuma destas regras são aplicáveis se os dados pessoais forem alvo de tratamento ilícito.

O controlo e supervisão do cumprimento das regras sobre a proteção de dados na Alemanha, está a cargo do Comissário Federal para a Proteção de Dados e a Liberdade de Informação. O Comissário goza de total independência no exercício das suas funções e desempenho das suas competências, devendo, para o efeito, permanecer livre de influência externa, direta ou indireta, e não aceita ou solicita instruções a ninguém. No entanto, fica sujeito ao controlo do Bundesrechnungshof³⁵, desde que tal não afete a sua independência³⁶.

³⁵ Tribunal Federal de Contas.

³⁶ Capítulo IV, secção 10, n.ºs 1 e 2 de Lei Federal de Proteção de Dados,

4.1.2. Espanha

Espanha tem acompanhado a evolução tecnológica e conseqüentemente, a evolução da matéria respeitante à proteção de dados pessoais, com especial enfoque, na figura do trabalhador e no direito de privacidade.

A par de outros ordenamentos jurídicos europeus, a matéria da proteção de dados na Espanha é regulada em termos de regulação comunitária, pelo RGPD. Além disso, Espanha tem tido avanços bastante significativos, sendo que o principal diploma nesta matéria é a *Ley Orgánica 3/2018*, de 5 de dezembro, destinada à Proteção de dados pessoais e garantia dos direitos digitais, doravante, LOPDGDD.

4.1.2.1. Percurso para a legislação sobre a proteção de dados na Espanha

Previamente a entrada em vigor da LOPDGDD, vários outros diplomas legais em matéria de dados foram aprovados, entre os quais, a Lei Orgânica de Regulamentação do Tratamento Automatizado de Dados Pessoais, doravante, LORTAD, em 1992, a Lei Orgânica 15/1999, de 13 de dezembro, Lei de Proteção de Dados Pessoais, doravante, LOPRODA, para acomodar a Diretiva 95/46/CE e superar a LORTAD, tendo desta forma expandindo o âmbito de aplicação, uma vez que era aplicável quer ao processamento de dados automatizados, quer de dados não automatizados. No seguimento da LOPRODA, foi aprovado o Real Decreto 1720/2007, de 21 de dezembro, que aprova o Regulamento para o desenvolvimento da Lei Orgânica 15/1999, de 13 de dezembro³⁷, sobre a proteção de dados, concedendo ao titular dos dados direitos como o acesso, retificação e cancelamento de dados, não estava ainda consagrado o direito ao apagamento dos dados, ou direito a ser esquecido, pese embora, com o recurso ao direito ao cancelamento de dados seria possível o alcançar o direito ao apagamento dos mesmos.

Por conseguinte, quanto ao direito ao esquecimento especialmente consagrado para o trabalhador, também não se encontrava expressamente consagrado, razão pela qual acreditamos que, o trabalhador que quisesse ver esquecidos ou apagados os seus dados pessoais, também teria de recorrer a outras normas e aos direitos que expressamente consagrados para fundamentar a sua pretensão.

³⁷ Seguimos de perto Suárez. Arturo Montesdeoca, De la protección de datos personales a la construcción de un catálogo de derechos digitales de las personas trabajadoras, ob.cit., pp. 153-167.

4.1.2.2. Lei Orgânica 3/2018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e Garantia dos Direitos Digitais, doravante, LOPDGDD

A LOPDGDD tem por objeto a execução no sistema jurídico espanhol do RGPD, bem como a salvaguarda do direito fundamental das pessoas singulares à proteção de dados pessoais protegido pelo n.º 4 do artigo 18.º da Constituição espanhola, que estabelece que, a lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos, direito este que deve ser exercido em conformidade com as disposições previstas no RGPD e na LOPDGDD.

Apesar de serem diplomas estritamente conectados, uma vez que um é pode ser considerado razão de ser do outro, entre o RGPD e a LOPDGDD, existem diferenças muito relevantes, entre as quais, o facto de a LOPDGDD, contrariamente ao que acontece noutros OJ, não ser apenas uma lei de execução do RGPD em Espanha mas, também é uma inovação do que respeita ao direito da privacidade, em especial, à privacidade do trabalhador bem como aos direitos digitais do cidadão em geral.

Quanto ao âmbito de aplicação, nos termos do artigo 2.º, a presente lei aplica-se a qualquer tratamento de dados total ou parcialmente automatizado, bem ao tratamento de dados pessoais não automatizados, contidos ou destinados a ser incluídos num ficheiro, estando essa aplicabilidade limitada aos títulos I a IX e artigos 89.º a 94 da lei. Assim, está excluído o título X, referente à garantia dos direitos digitais, com a exceção dos artigos 89.º a 94.³⁸ desse mesmo título.

Quanto ao direito à privacidade previsto na LOPDGDD, estabelece o artigo 87.º deste diploma legal, com a epígrafe *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral* que, os trabalhadores e empregados públicos têm direito à proteção da sua privacidade na utilização de dispositivos digitais colocados à sua disposição pelo empregador, ou seja, independentemente dos dispositivos em questão serem propriedade do empregador, é sempre exigido a esse o respeito pela privacidade do trabalhador. Acrescenta por isso o n.º 2 que, o empregador pode ter acesso aos conteúdos derivados da utilização de meios digitais fornecidos

³⁸ O artigo 89.º é referente ao direito à privacidade face à utilização de dispositivos de videovigilância e de registo de som no local de trabalho. O art.º 90 é referente ao Direito à privacidade na utilização de sistemas de geolocalização no local de trabalho. O art.º 91.º é referente aos Direitos digitais na negociação coletiva. O art.º 92.º Referente à proteção de dados de menores na internet. O art.º 93.º Referente ao Direito a ser esquecido nas pesquisas na internet. E o art.º 94.º referente ao direito a ser esquecido nos serviços de redes sociais e serviços equivalentes.

aos trabalhadores com o único objetivo de controlar o cumprimento de obrigações decorrentes do contrato de trabalho ou estatutos e garantir a integridade de tais dispositivos, nunca com objetivo de interferir nas questões pessoais que respeitem ao trabalhador, para que isso seja possível, é exigido aos empregadores que tomem determinadas medidas, estabelecendo o n.º 3 que, o empregador deve estabelecer critérios para a utilização de dispositivos digitais, respeitando em todo o caso as normas mínimas de proteção da sua privacidade de acordo com os costumes sociais e os direitos constitucionalmente e legalmente reconhecidos. Os representantes dos trabalhadores devem estar envolvidos na elaboração destas normas. Assim, podemos concluir que, se estando na posse do trabalhador um dispositivo digital fornecido pelo empregador, o trabalhador terá total controlo da informação pessoal que colocar no dispositivo, podendo, livremente, apagar, corrigir e aceder à referida informação a todo o tempo.

No que diz respeito ao direito ao esquecimento, o artigo 15.º estabelece que o direito ao apagamento deve ser exercido em conformidade com o disposto no artigo 17.^{o39} do RGPD. Este artigo estabelece ainda que, quando o apagamento resultar do exercício do direito de oposição nos termos do art.º21.º, n.º2⁴⁰ do RGPD, o responsável pelo tratamento pode conservar os dados de identificação da pessoa em causa necessários para impedir o tratamento futuro para efeitos de comercialização direta.

Adicionalmente, esta lei prevê duas situações específicas em que se pode exercer o direito ao esquecimento, nomeadamente, no art.º93.º referente ao direito a ser esquecido das pesquisas na internet, onde é concedido ao titular dos dados o direito a que os motores de busca da internet suprimam os resultados obtidos através da pesquisa efetuada com base no nome, as ligações publicadas que contenham informações relativas a essa pessoa, se forem inadequadas, inexatas, irrelevantes, desatualizadas ou excessivas ou que assim se tornem com o passar do tempo, tendo em conta os fins para os quais foram recolhidos ou tratados, o tempo decorrido e a natureza, bem como o interesse público da informação. O mesmo aplicar-se-á, quando as circunstâncias pessoais do titular dos dados demonstrem que os seus direitos prevalecem sobre a manutenção das ligações pelo serviço de pesquisa na internet. No mesmo sentido vai o art.º94.º, por sua vez, referente ao direito a ser esquecido nos serviços de redes sociais e serviços equivalentes.

³⁹ Referente ao direito ao apagamento de dados (“direito a ser esquecido”).

⁴⁰ *Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.*

Quanto ao direito ao esquecimento aplicado à figura do trabalhador, a lei nada prevê expressamente, no entanto, estipula direitos referentes ao respeito pela vida privada, intimidade e privacidade, pelo que, o direito ser-lhe-á aplicado, à partida, com recurso a estas normas, bem com os artigos 15.º, 93.º e 94.º (consoante dos casos), da LOPDGDD, em harmonia com o artigo 17.º RGPD.

O controlo do cumprimento e a efetivação das normas constantes do RGPD, bem como da LOPDGDD cabe à Agência Espanhola de Proteção de Dados, que é uma autoridade administrativa independente com personalidade jurídica e plena capacidade pública e privada, que atua com total independência dos poderes públicos no exercício das suas funções.

Desta forma, nos termos do artigo 47.º da LOPDGDD, compete a esta agência a supervisão e aplicação da lei orgânica do RGPD e em particular, exercer as funções estabelecidas no artigo 57.º, que respeita às atribuições das autoridades de controlo territoriais em cada EM a que o RGPD é aplicável, bem como os poderes de investigação estabelecidos no artigo 58.º do mesmo regulamento.

4.2. Ordenamentos jurídicos de expressão portuguesa

4.2.1. Cabo Verde

O ordenamento jurídico cabo-verdiano já percorreu um longo caminho em matéria de proteção de dados pessoais. Diversas modificações legislativas e socioeconómicas do país permitiram que a matéria da proteção de dados pessoais em Cabo Verde hoje esteja devidamente regulamentada.

Desde a sua génese, a lei de proteção de dados cabo-verdiana, diz respeito à aplicação ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meio não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados. Tratamento esse que deve respeitar diversos princípios previsto na legislação, sendo que o princípio geral a ser respeitado diz respeito ao processamento dos dados, que deve efetuar-se no estrito respeito pelos direitos, liberdades e garantias fundamentais das pessoas singulares, em especial pelo direito à reserva da intimidade da vida privada e familiar e pelo direito à proteção de dados pessoais.

Por conseguinte, o percurso em busca de uma maior e melhor regulamentação nesta matéria em Cabo Verde, começou com a Lei n.º 133/V/2001, de 22 de janeiro, que aprovou o regime jurídico geral de proteção de dados pessoais em Cabo Verde (Lei da Proteção de Dados Pessoais Cabo-verdiana ou Lei da proteção de Dados), com as alterações introduzidas pela Lei n.º 41/VIII/2013, de 17 de setembro e mais recentemente pela Lei n.º 121/IX/2021, de 17 de março.

A Lei n.º 133/V/2001, tem como fonte direta a Lei n.º 67/98, de 26 de outubro Portuguesa, que, por seu turno, transpôs para a ordem jurídica portuguesa a Diretiva 95/46/CE, e ainda a Convenção 108 do Conselho da Europa, da qual Cabo Verde é parte desde 1 de outubro de 2018⁴¹. Por outro lado, a mais recente alteração, através da Lei 121/IX/2021, de 17 de março é muito inspirada pelo RGPD, sendo que esta nova lei veio implicar mudanças profundas no paradigma regulatório da matéria e com impactos significados na atividade económica e empresarial da sociedade cabo-verdiana, incluindo novos conceitos, como a pseudonimização, dados biométricos, violação de dados pessoais, dados relativos à saúde e definição de perfis.

Foram ainda inseridos os direitos de retificação e apagamento, direitos estes que já vinham inseridos na legislação anterior embora incluídas numa das alíneas do “Direito ao acesso”, o

⁴¹ Crf. Ponto 1. Preâmbulo da Lei n.º 121 /IX//2021 de 17 de março.

que fazia com que se presumisse se tratar de direitos cujo exercício pressuporia necessariamente o acesso aos dados. Porém, em termos práticos, os direitos de retificação e apagamento são direitos que podem ser exercidos sem implicar a invocação do direito de acesso, dito de outra forma, os mesmos podem ser exercidos autonomamente⁴². Exatamente por serem direitos autónomos, com a mais recente alteração, foram incluídos em artigos próprios, assim, o artigo 15.º é dedicado ao direito de retificação, concedendo ao titular dos dados o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Por seu turno, o artigo 16.º dedicado ao direito ao apagamento, concede ao titular dos dados o direito de obter do responsável pelo tratamento o apagamento ou a destruição dos seus dados pessoais, sem demora injustificada, e ao responsável pelo tratamento, a obrigação de os apagar, sem demora injustificada, nos casos em que deixem de ser necessários para a finalidade que motivou a recolha, o titular retirar o consentimento, se não existir outro fundamento jurídico para o tratamento, ou no caso de oposição ao tratamento e não existam interesses legítimos que prevaleçam que justifiquem o tratamento, ou seja, haverá sempre a necessidade de ponderar os interesses em causa, pelo que este direito não poderá ser exercido de forma absoluta, o mesmo aplicar-se-á quando estivermos perante uma relação laboral, trabalhador/empregador.

A fiscalização da proteção de dados pessoais em Cabo Verde é assegurada pela Comissão Nacional de Proteção de Dados (CNPd), que funciona junto da Assembleia Nacional, que é regulada pela Lei n.º 42/VIII/2013, de 17 de setembro. O artigo 8.º, n.º 1 desta última lei referente às atribuições da CNPD, estabelece que esta é uma autoridade nacional à qual incumbe controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos humanos e pelas liberdades e garantias consagradas na Constituição e na lei. A CNPD exerce as suas competências em todo o território cabo-verdiano e coopera com as autoridades de controlo de proteção de dados pessoais de outros Estados na difusão do direito nessa matéria, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro⁴³.

Em termos civis, o artigo 47.º da lei de proteção de dados cabo-verdiana estabelece que (1) qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições legislativas ou regulamentares em matéria de proteção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo causado. E

⁴² Ponto 13 do preâmbulo da Lei 121/IX/2021, de 17 de março.

⁴³ Artigo 4.º, números 1 e 3 da Lei n.º 42/VIII/2013, de 17 de setembro.

acrescenta (2) que o responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano não lhe é imputável.

4.2.2. Moçambique

Moçambique e Portugal, têm vindo a desenvolver relações em diversas frentes, no entanto, e apesar de em termos legislativos estes ordenamentos jurídicos serem bastante semelhantes e Moçambique ter vindo a acompanhar Portugal em diversas matérias no âmbito da legislação constitucional, comercial, laboral, entre outros, o mesmo não se pode dizer no que se refere à matéria de proteção de dados pessoais. Isto porque, não existe ainda regulação nacional sobre esta matéria no ordenamento jurídico moçambicano. Desta forma, no que se refere à proteção de dados pessoais e à entidade reguladora e fiscalizadora do cumprimento de normas sobre esta matéria, o ordenamento jurídico moçambicano tem uma lacuna a preencher.

Recorre-se, por isso, a outros diplomas legislativos. Assim, tendo em consideração que nos termos da Constituição da República de Moçambique (CRM), *“todo o cidadão tem direito à honra, ao bom nome, à reputação, à defesa da sua imagem e à reserva da sua vida privada”*⁴⁴, a salvaguarda e proteção de dados pessoais está prevista de modo muito geral no artigo 71.º da CRM, com a epígrafe *“utilização da informática”*, onde no seu n.º 1 proíbe expressamente *“a utilização de meios informáticos para registo e tratamento da dados individualmente identificáveis relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical e à vida privada”*. Complementarmente, o n.º 2 do mesmo artigo remete para a lei a regulamentação da proteção de dados pessoais constantes de registos informáticos, as condições de acesso aos bancos de dados, a constituição e utilização por autoridades públicas e entidades privadas destes bancos de dados ou de suportes informáticos, regulamentação esta que, tal como oportunamente referido, ainda não foi aprovada. Os números 3 e 4, referem-se à proibição de acesso e transferência dos dados, ao direito de acesso e a retificação pelo titular dos dados.

Além da Constituição da República de Moçambique, a Lei das Transações Eletrónicas, Lei n.º 03/2017, de 9 de janeiro, estabelece normas sobre a proteção de dados pessoais, embora apenas para o sector específico das transações eletrónicas. Esta lei tem como objeto estabelecer os princípios, normas gerais e o regime jurídico das transações eletrónicas em geral, do comércio eletrónico em particular, visando garantir a proteção e utilização das tecnologias de informação e comunicação⁴⁵. Assim a lei das transações eletrónicas vem estabelecer, para o sector das transações eletrónicas, normas sobre proteção de dados eletrónicos pessoais, nomeadamente,

⁴⁴ Artigo 41.º da Constituição da República de Moçambique.

⁴⁵ Artigo 1.º da Lei n.º 03/2017, de 9 de janeiro.

normas sobre as obrigações do processador de dados, proibição de acesso e de transferência e responsabilidade do processador de dados, com a exceção do processamento, recolha ou divulgação eletrónica de dados pessoais para efeitos de jornalismo, expressão artística, literária ou quando decidido pelas autoridades competentes para a salvaguarda da segurança pública e defesa nacional⁴⁶.

Adicionalmente, Moçambique ratificou, através da Resolução n.º 5/2019, de 20 de junho, a Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, de 27 de junho de 2014, relativa à criação de um quadro jurídico sobre a Cibersegurança e Proteção de Dados Pessoais, incorporando os compromissos existentes dos Estados Membros da União Africana no plano sub-regional, regional e internacional, de construção da Sociedade de Informação. Nesta Convenção, cada Estado Parte compromete-se a criar um quadro jurídico, tendo como objetivo reforçar os direitos fundamentais e liberdades públicas, nomeadamente, a proteção de dados físicos, e reprimir qualquer infração relativa à vida privada, sem prejuízo da liberdade de circulação de dados pessoais⁴⁷. Mais, cada Estado Parte está obrigado ao dever de criar uma autoridade responsável pela proteção de dados pessoais⁴⁸, o que não aconteceu em Moçambique.

Com tudo o que foi exposto, é inequívoco afirmar que, embora todos os avanços legislativos a nível mundial e consequente urgência na regulação da matéria da proteção de dados pessoais, bem assim do direito ao esquecimento em termos gerais e, aplicado ao trabalhador, o impulso de outros ordenamentos jurídicos próximos, e ao compromisso aceite através da Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, Moçambique não acompanhou este desenvolvimento uma vez que não executou as normas sobre esta matéria na legislação nacional. Dito isto, para responder a violações relativas a proteção de dados pessoais, o ordenamento jurídico moçambicano terá de recorrer a normas constitucionais e civis, quer pela falta de legislação nacional, quer pela inexistência de uma entidade independente com competência exclusiva de controlo do cumprimento de normas relativas a proteção de dados pessoais no território moçambicano.

⁴⁶ Artigo 65.º, n.º 5 da Lei n.º 03/2017, de 9 de janeiro.

⁴⁷ Artigo 8.º, n.º 1 da Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, de 27 de junho de 2014.

⁴⁸ Artigo 11.º, n.º 1, alínea a) da Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, de 27 de junho de 2014.

CAPÍTULO III – DA PROTEÇÃO DE DADOS PESSOAIS AO DIREITO A SER ESQUECIDO

5. Relevância da regulamentação da matéria de proteção de dados e do direito ao esquecimento

5.1. Definição de conceitos-chave

O estudo da matéria relativa à proteção de dados pessoais e o direito ao esquecimento exige a compreensão de alguns conceitos. Para o presente estudo, os conceitos de dados pessoais, dados biométricos, tratamento de dados, responsável pelo tratamento e consentimento, têm especial relevância. Posto isto, nos termos do artigo 4.º com recurso do RGPD, entende-se por:

1. Dados pessoais – a informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); neste preceito, esclarece-se ainda que, é considerada identificável uma pessoa 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.
2. Dados biométricos – consiste nos dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente, imagens faciais ou dados dactiloscópicos.
3. Tratamento dos dados – considera-se tratamento de dados pessoais a operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjunto de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.
4. Responsável pelo tratamento – considera-se responsável pelo tratamento dos dados pessoais a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse

tratamento sejam determinados pelo direito da união ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

5. Consentimento – o consentimento do titular dos dados representa uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

5.2. Da importância do direito da proteção de dados pessoais

Numa perspetiva mais ampla, podemos depreender que o direito da proteção de dados pessoais deve ser entendido como o conjunto sistematizado de princípios, normas e institutos que regula os dados pessoais e o seu tratamento⁴⁹. Apesar de o direito da proteção de dados não ser um ramo jurídico novo, apenas recentemente assumiu uma importância indiscutível no panorama jurídico económico nacional, europeu e internacional.

Segundo A.Barreto Menezes Cordeiro⁵⁰, a importância do direito da proteção de dados advém, sobretudo, do impacto social, numa aceção amplíssima, do tratamento de grandes quantidades de dados (*Big Data*), sem propósitos exaustivos. Numa perspetiva específica, ou seja, focada apenas no direito da proteção de dados, esta matéria assume uma importância incontestável no quotidiano das pessoas comuns. Assim, o crescimento exponencial do tratamento automatizado de dados, espoletado pelos avanços tecnológicos das últimas décadas, coloca-nos, a todos, numa posição de enorme fragilidade: as informações pessoais hoje armazenadas, pelos mais distintos responsáveis pelo tratamento, públicos e privados, são hoje superiores às informações que nós próprios detemos sobre a nossa vida. Ora, o panorama descrito não corresponde a uma realidade jovem, tem acompanhado a evolução da sociedade contemporânea de forma particularmente evidente. O RGPD apenas colocou os dados pessoais e o seu tratamento no centro das preocupações jurídicas empresariais. Preocupação essa que se multiplica no âmbito das relações laborais.

A emergência do direito da proteção de dados surge como um reflexo da revolução trazida pelo RGPD, com destaque para a densificação dos direitos dos titulares de dados pessoais, o

⁴⁹ Seguimos de perto o autor Cordeiro, A.Barreto Menezes (2020), *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, p.35.

⁵⁰ Cordeiro, A.Barreto Menezes (2020), *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, ob. cit., pp. 28-29.

agravamento dos deveres dos responsáveis pelo tratamento e dos subcontratantes, bem como o reforço das competências das autoridades do controlo e a obrigatoriedade de designação de encarregado de proteção de dados.

O direito da proteção de dados assume-se, assim, como um ramo jurídico eclético, que pressupõe uma constante interação entre o Direito privado e o Direito Público, o Direito português e o Direito europeu. A produção legislativa relativa aos dados pessoais justifica-se não apenas para acautelar os interesses individuais dos titulares de dados, uma vez que esses seriam sempre protegidos através da invocação de normas gerais relativas aos direitos de personalidade, mas sim, para regular o seu tratamento⁵¹.

“A regulação específica e autónoma do tratamento de dados pessoais surge como uma resposta à utilização de mecanismos automatizados no processamento de informação pessoal. Os avanços tecnológicos (elemento objetivo) e as vantagens decorrentes dessa evolução (elemento subjetivo) impeliram tanto o sector público o sector privado e intensificaram o tratamento dos dados pessoais. As razões que motivaram o interesse destes dois sectores são distintas. No sector público, o tratamento automatizado apresentou-se como uma solução quotidiana indispensável em face do crescimento da administração pública, fruto da disseminação das agências federais (EUA) ou da assunção de um modelo de Estado Social (Europa). No sector privado, o tratamento automatizado assumiu um papel transversal: na relação com os clientes, na gestão de *stocks*, na identificação de riscos de incumprimento, no posicionamento no mercado ou na determinação das estratégias de *marketing* e de publicidade”⁵².

Nas relações laborais, o tratamento automatizados de dados pessoais surge desde o momento pré-contratual, permanecendo na fase contratual e se alargando para o período pós-contratual. Em qualquer uma das fases, o tratamento de dados deve se orientar por normas legais relativas ao tratamento dos mesmos, de modo a salvaguardar a privacidade e segurança jurídica do titular dos dados pessoais, que no caso das relações laborais será o trabalhador, o candidato a emprego ou antigo trabalhador - quando o tratamento de dados se mostre necessário e legítimo mesmo quando a relação jurídico-laboral já tenha chegado ao fim, por cessação do contrato de trabalho. No entanto, as normas referentes ao direito ao esquecimento, se, e na medida em que se mostrar aplicável ao caso concreto, poderão ser aplicadas em cada uma dessas fases.

⁵¹ Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019, p. 33, Almedina, 2020.

⁵² Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019, p. 37, Almedina, 2020.

6. Relevância do direito ao esquecimento no direito do trabalho

6.1.O Conceito do direito ao esquecimento

O direito ao esquecimento pode ser definido como um “direito fundamental de personalidade amparado no princípio da dignidade humana, segundo o qual, uma pessoa individual ou coletiva, tem o direito à autodeterminação informativa, isto é, pode requerer o apagamento, retirada ou bloqueio da divulgação de dados, lícitos ou não, que lhe digam respeito, encontrados nos diversos meios de comunicação e que não tenham mais interesse público, judicial, histórico ou estatístico ou ainda que não sejam vedados por lei. Não se trata, portanto, de eliminar todas as referências a factos ocorridos no passado, mas apenas de evitar a exposição desnecessária e lesiva de acontecimentos desprovidos de interesse público atual. Exprime, em suma, um poder de autocontrolo dos próprios dados pessoais”⁵³.

Assim, a ideia jurídica da figura do direito ao esquecimento reside na proteção da vida privada e intimidade das pessoas, bem como a reabilitação e a ressocialização dos indivíduos, que seriam impedidas ou consideravelmente dificultadas pela lembrança indefinida dos factos cometidos. O direito ao esquecimento pode assim ser considerado um desmembramento do direito à reserva da intimidade da vida, previsto no artigo 80.º do Código Civil, relativo à reserva sobre a intimidade da vida privada.

De forma expressa, nos seus considerandos 65 e 66, o RGPD faz alusão ao direito ao esquecimento.

Assim, o considerando 65 prevê que “os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o “direito a serem esquecidos” quando a conservação desses dados violar o RGPD ou o direito da união ou dos Estados Membros aplicável ao Responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento dos dados pessoais que lhes digam respeito ou se o tratamento dos dados pessoais não respeitar o disposto no RGPD. Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais

53 Ataíde, Rui Paulo Mascarenhas (2019), “Direito ao esquecimento”, in Cyberlaw, Vol. 1, n.º7, p. 16.

tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto e o consentimento ter sido efetuado na sua infância. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.”⁵⁴.

Por seu turno, o considerando 66 do RGPD prevê que “para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao apagamento deverá ser alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adotar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados.”⁵⁵. Pensemos, por exemplo, numa empresa do setor imobiliário que divulga a imagem e o currículo dos seus consultores no seu website. Quando a relação jurídico-laboral entre a referida empresa e determinado colaborador cessar, independentemente do motivo da cessação, o responsável pelo tratamento, no caso, o empregador, sem demora injustificada, deverá tomar as medidas técnicas necessárias para a supressão das ligações relativas aos dados do colaborador em questão, uma vez que a finalidade para qual os dados foram recolhidos deixou de existir. Haverá, no entanto, a necessidade de analisar situações onde se aplicam as exceções à regra.

⁵⁴ Considerando 65 do RGPD.

⁵⁵ Considerando 66 do RGPD.

6.2.Direito ao apagamento dos dados («direito a ser esquecido») nos termos do artigo 17.º do RGPD

Posto isto, nos termos do artigo 17.º, n.º1 do RGPD, o titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) os dados pessoais deixarem de ser necessários para a finalidade que motivou a sua recolha; b) o titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º1, alínea a)⁵⁶, ou do artigo 9.º, n.º 2, alínea a)⁵⁷ e se não existir outro fundamento jurídico para o referido tratamento; c) o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1⁵⁸, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2⁵⁹; d) os dados pessoais foram tratados ilicitamente; e) os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União e de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) os dados pessoais são recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º1⁶⁰.

Por seu turno, o n.º 2 do artigo 17.º estabelece que, “Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º1, toma as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia

⁵⁶ Artigo 6.º, n.º1 do RGPD “ O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) o titular dos dados tiver dado seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.”

⁵⁷ Artigo 9.º, n.º 2 do RGPD - O disposto no n.º1 (referente à proibição do tratamento de determinadas categorias de dados pessoais) não se aplica se se verificar um dos seguintes casos: a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados.

⁵⁸ “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, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 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 declaração, exercício ou defesa de um direito num processo judicial”.

⁵⁹ “Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta”.

⁶⁰ “Quando for aplicável o artigo 6.º, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança”.

disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos”.

Assim, nos termos do n.º 2, o direito ao esquecimento pressupõe o preenchimento cumulativo de dois elementos: (i) o responsável pelo tratamento tiver tornado públicos os dados pessoais em causa; e (ii) for obrigado a apagá-los, por determinação do n.º 1.

Neste contexto, o primeiro elemento decompõe-se em dois requisitos: (i) ter sido o próprio responsável pelo tratamento a divulgar a informação; *a contrário* quando não tiver sido, o titular nada lhe pode exigir; e (ii) ter tornado os dados públicos, i.e., disponibilizado os dados a um número indeterminado de sujeitos.

O RGPD não exige que essa divulgação tenha sido realizada via *internet*, conquanto corresponda ao caso padrão⁶¹. Por seu turno, quanto ao segundo elemento, importa notar que, a emergência do direito ao esquecimento apenas ocorrerá na medida em que o titular possa exigir o apagamento dos dados, nos termos do n.º 1. Ou seja, sem essa subsunção do caso concreto a uma dessas alíneas, não pode o titular dos dados invocar o artigo 17.º, n.º 2, pelo que, o direito ao apagamento dos dados, ou direito a ser esquecido, não tem carácter absoluto, devendo sempre ser feita a subsunção da norma ao caso em concreto e em conformidade com o princípio da proporcionalidade.

Por fim, o n.º3 do mesmo artigo alude aos casos em que o direito ao esquecimento não se aplicará, estando na génese desta proibição as situações de conflitos de direitos. Assim. Nos termos do n.º3, os números 1 e 2 não se aplicam na medida em que o tratamento se revele necessário: a) ao exercício da liberdade de expressão e de informação; b) ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º2, alíneas

⁶¹ Cordeiro, A. Barreto Menezes (2020), *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, pp. 280-281.

h)⁶² e i)⁶³, bem como do artigo 9.º, n.º 3⁶⁴; d) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1⁶⁵, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

6.3.A natureza jurídica e o exercício efetivo do direito ao esquecimento

O debate sobre a natureza jurídica do direito ao esquecimento ainda não está fechado. Contudo, a doutrina majoritária tem defendido que este direito faz parte do leque dos direitos de personalidade. Desta feita, como uma extensão dos direitos de personalidade já consagrados, sobretudo, através do direito à intimidade da vida privada, à identidade pessoal, à honra e ao bom nome, sendo que alguns destes direitos já foram elevados à categoria de direitos fundamentais constitucionalmente consagrados, conforme o artigo 26.º da CRP.

Partindo da premissa de que a personalidade jurídica das pessoas singulares adquire-se, nos termos do n.º 1 do art.º 66.º do CC, no momento do nascimento completo e com vida, cessando a mesma personalidade, nos termos do n.º 1 do art.º 68.º CC, com a morte, e sem prejuízo da tutela de direitos de personalidade de pessoa falecida, nos termos do artigo 71.º CC, o direito ao esquecimento, em termos gerais, à partida, também será adquirido nesse exato momento,

⁶² “Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3”.

⁶³ “Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional”.

⁶⁴ “Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes”.

⁶⁵ “O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo”.

enquanto indivíduo que dota de personalidade jurídica, e se expandirá com o decurso da vida, nas relações jurídicas e nos contratos que o indivíduo celebrará ao longo da sua vida, incluindo o contrato de trabalho.

Assim, ao prestar o consentimento para o tratamento dos seus dados pessoais, que inevitavelmente terá de o fazer, por exemplo, aquando da celebração de um contrato de trabalho, transferindo a responsabilidade para o tratamento dos seus dados pessoais ao empregador, o trabalhador coloca à disposição do empregador a responsabilidade pelo tratamento dos direitos de personalidade que assistem no âmbito daquela relação laboral. Assim, quando por algum motivo este tratamento não se mostre mais necessário, é a este responsável pelo tratamento que o trabalhador deverá recorrer quando posteriormente e com fundamentos legítimos entender que o tratamento por algum motivo se mostre desnecessário ou contrário às finalidades para as quais os dados foram recolhidos.

A natureza jurídica do direito ao esquecimento, que está prevista no n.º2 do artigo 17.º, suscita dúvidas. “Segundo a letra do preceito, o direito ao esquecimento não consiste num direito a exigir, do público em geral, o apagamento de determinados dados pessoais, mas somente no direito a exigir ao responsável pelo tratamento que informe os demais responsáveis de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como o apagamento de eventuais cópias ou reproduções. A comunicação desta intenção não parece sequer fazer emergir na esfera jurídica desses outros responsáveis pelo tratamento uma obrigação (passiva) de apagamento: cabe ao titular dos dados requerê-lo individualmente”⁶⁶.

Os responsáveis pelo tratamento, independentemente de lhes ser dirigido um pedido para apagarem determinados dados pessoais, diretamente pelo titular ou indiretamente pelo responsável pelo tratamento a quem foi dirigido um pedido nos termos do artigo 17.º, n.º2, devem sempre atuar no estrito cumprimento, entre outros, do princípio da minimização dos dados e do princípio da limitação da conservação. Nesse sentido, a obrigação de apagar existirá sempre. O que não parece existir é uma obrigação específica para com o titular de dados que requeira a comunicação da intenção de ver uma determinada informação esquecida do espaço digital. O direito ao esquecimento apenas permite acelerar o apagamento desses dados. De resto, é perfeitamente possível que em relação a um ou mais desses responsáveis pelo tratamento sejam aplicáveis algumas das exceções elencadas no n.º3. A comunicação da intenção do titular

⁶⁶ Cordeiro, A. Barreto Menezes (2020), Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019, pag.275.

dos dados abrange todos os *links*, cópias e reproduções relativas à informação que se pretende ver esquecida.

Desta forma, o direito ao esquecimento surge como um reconhecimento da insuficiência do apagamento dos dados pelo responsável pelo tratamento originário, em face das especificidades da *internet*⁶⁷. No entanto, o RGPD, na letra do artigo 17.º não obriga que tal divulgação seja realizada através da internet, caso contrário se veria esvaziado o efeito útil do preceito.

Ora, uma vez verificados os elementos do n.º 2, anteriormente decompostos, deve o responsável pelo tratamento, mediante a apresentação pelo titular visado, de um pedido nesse sentido, informar (i) os responsáveis pelo tratamento efetivo dos dados pessoais do pedido formulado pelo titular, (ii) recorrer às medidas que forem razoáveis, atendendo à tecnologia disponível e aos custos da sua aplicação. Sendo que ao responsável pelo tratamento não cabe garantir o apagamento dessa informação, mas apenas participar aos demais responsáveis pelo tratamento efetivo⁶⁸. Dificilmente conseguirá o responsável pelo tratamento originário identificar ou comunicar com todos os responsáveis efetivos – incluindo os que se encontrem fora do espaço da UE, o que suscita dúvidas quanto à forma pelo qual o pedido do titular deva ser difundido. De todo o modo, espera-se que o tente fazer, recorrendo às medidas necessárias, sem assumir custos excessivos e atendendo às consequências decorrentes da conservação pública dessa informação para o titular dos dados visado.

Não sendo possível identificar todos os responsáveis efetivos, alguma doutrina sugere que o responsável divulgue o pedido do titular no sítio onde a informação constava inicialmente. No entanto, esta solução causa algumas dúvidas, visto que dificilmente será possível divulgar esse pedido sem dar a conhecer precisamente a informação que se pretende apagar.

⁶⁷ Paal, Anotação ao artigo 17.º do RGPD em Paal/Pauly, Rn. 8; Considerando 66, p. 1: apresenta o direito ao esquecimento como uma forma de reforçar o direito ao apagamento *lato sensu* e *stricto sensu*.

⁶⁸ Cordeiro, A. Barreto Menezes (2020), Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019, pag.281.

6.4.O direito ao esquecimento nas relações laborais

Do enquadramento da matéria do direito ao esquecimento acima, torna-se necessário subsumir esta matéria às relações laborais. Desta forma, importa responder algumas questões, nomeadamente, se este direito poderá ser aplicável ou não neste tipo de relações jurídicas e em que medida.

Como anteriormente exposto, o direito ao esquecimento pode ser entendido como um direito fundamental, estritamente ligado ao direito à vida privada e aos demais direitos de privacidade, como o bom nome, honra, intimidade, etc.

Assim, ao começar uma relação laboral, a pessoa (o trabalhador), inevitavelmente traz consigo todos os direitos fundamentais e direitos de personalidade inerentes a sua condição de pessoa e, enquanto trabalhador, irá acrescentar os demais direitos que a lei garante como trabalhador, que reflete não apenas na execução do próprio contrato de trabalho, mas também na organização a que se vai inserir⁶⁹. Razão pela qual concluímos que este direito é merecedor de tutela jurídica a par com os demais direitos de personalidade do trabalhador.

O direito ao esquecimento nas relações laborais poderá ser aplicável em três fases, nomeadamente, na fase pré-contratual, contratual e pós-contratual, sendo que será necessário a adoção de medidas que assegurem que a informação de cariz pessoal e os dados pessoais que um empregador detém sobre os seus trabalhadores, seja apagada quando a finalidade para a qual foram recolhidos deixar de existir.

Adicionalmente, o art.º 88.º, n.º1 do RGPD, estabelece a possibilidade de os EM, nos seus OJ, ou em convenções coletivas, estabelecerem normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no OJ ou em convenções coletivas, de gestão, planeamento e organização de trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção de bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação laboral.

⁶⁹ Studart, Ana Paula Didier & Martinez, Luciano (2019), O Direito ao Esquecimento como Direito fundamental nas relações laborais, p. 137.

Segundo Simão Sant’Ana⁷⁰, “com a cessação do contrato de trabalho esgota-se a finalidade para a qual o empregador até então processava os dados do trabalhador, mas não deverá o empregador proceder ao apagamento imediato de tais dados uma vez que o trabalhador tem até um ano para impugnar o seu despedimento, pelo que, será da mais elementar prudência guardar tais dados pelo menos um ano após a cessação do contrato de trabalho, sem prejuízo de outros prazos particularmente aplicáveis a matérias concretas como o registo das horas de trabalho ou aos processos de seleção e recrutamento, casos em que a própria lei estipula um prazo de conservação de cinco anos”. E acrescenta que, o esgotamento da finalidade da recolha dos dados terá de ser articulado com o prazo legal aplicável ao cumprimento da obrigação de retenção de informação/documentação que recai sobre o empregador.

Não podemos esquecer que o direito ao esquecimento não é um direito absoluto, pelo que, ainda que no âmbito das relações laborais, haverá certamente importantes exceções onde o empregador tem a obrigação ou o direito de não apagar os dados do trabalhador, conforme também menciona o autor acima referido.

Ora, no que diz respeito a esta matéria, a legislação portuguesa, mais concretamente o CT, remete para a legislação de proteção de dados pessoais, conforme o artigo 17.º, n.º 4, que estabelece que os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à proteção de dados pessoais. Falta, por isso, clarificar o âmbito de aplicabilidade do direito ao esquecimento perante os diferentes titulares de dados, no caso em concreto, perante o trabalhador.

6.4.1. O direito ao esquecimento nas diferentes fases da relação laboral

O direito ao esquecimento nas relações laborais não pode ser aplicado de igual forma nas diferentes fases desta relação jurídica, isto porque os dados pessoais a serem facultados são diferentes em cada uma das fases. Regra geral, o início da relação entre o trabalhador enquanto titular dos dados e o empregador enquanto responsável pelo tratamento, é através da celebração de um contrato de trabalho, e o fim desta relação, é através da cessação do mesmo contrato de trabalho. No entanto, antes da celebração do contrato de trabalho, e depois da cessação do mesmo, existem dados pessoais do trabalhador em que o empregador é o responsável pelo

⁷⁰ As empresas e o novo RGPD: como ser-se “esquecido” do trabalho?, disponível em <https://eco.sapo.pt/2018/04/19/direito-a-ser-esquecido-ate-que-ponto-nos-podemos-apagar-da-internet/>

tratamento dos mesmos. A pensar nisso, será necessário averiguar em que medida será possível garantir ao trabalhador, nestes casos, o exercício do direito ao esquecimento.

No seguimento disso, no presente tópico, pretendemos analisar a possibilidade do exercício do direito ao esquecimento nas diferentes fases da relação laboral, particularmente, na fase pré-contratual, na figura do candidato ao emprego, na fase contratual, na figura do trabalhador, e a fase pós-contratual, na figura do ex-trabalhador.

Por conseguinte, há necessidade de, igualmente, delimitar o escopo dos dados pessoais destas figuras que poderão ser alvo de tratamento e, posteriormente, alvo do exercício do direito ao esquecimento por cada uma destas figuras, consoante a fase da relação laboral em que se encontrem. Desta forma, analisaremos, em relação a cada uma das fases, dados pessoais que: (1) nunca podem ser esquecidos; (2) podem sempre ser esquecidos; e (3) podem ser esquecidos, mas com algumas condicionantes.

6.4.1.1.O candidato ao emprego e o direito a ser esquecido

O candidato ao emprego, bem como o potencial empregador estão estritamente ligados à fase pré-contratual da formação do contrato de trabalho. Regra geral, o empregador, no uso da liberdade de iniciativa privada, prevista no artigo 61.º da CRP, mediante as necessidades da empresa, tem a liberdade de contratar. Liberdade essa que inclui a definição de requisitos eliminatórios do perfil dos candidatos a emprego para determinado posto de trabalho.

Geralmente, a contratação é precedida de um processo de recrutamento, processo esse em que os candidatos que considerem ter os perfis adequados a ocupar o referido posto de trabalho manifestam a sua vontade, comumente pelo envio de *Curriculum Vitae*, (doravante, CV), contendo nesse mesmo CV, diversas informações de carácter pessoal e profissional do candidato ao emprego. Fora ao CV, diversas empresas solicitam documentos e informações adicionais, como a carta de motivação, cartas de recomendação, testes de psicotécnicos, comprovativos de conhecimento de línguas estrangeiras e, em determinadas situações, é exigido ao candidato ao emprego o certificado de registo criminal, contudo, este documento não é de carácter obrigatório nesta fase, caso contrário, este requisito poderia constituir um requisito eliminatório e discriminatório para determinadas situações. Desta forma, o direito ao esquecimento é relevante para o candidato ao emprego. Imaginemos, por exemplo, que o candidato ao emprego tem antecedentes criminais e busca a ressocialização através do contrato de trabalho. Neste caso, o candidato tem todo o interesse em que os seus antecedentes criminais não sejam tidos em consideração, ou que seja esquecido em relação a tais factos, na verdade,

posterior utilização com o devido consentimento do titular. Contudo, se por alguma eventualidade tal não ocorrer, o candidato ao emprego terá o direito de exigir o apagamento dos mesmos nos termos previstos no artigo 17.º, al. a) do RGPD, ou seja, quando os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

Neste seguimento de ideias, quanto ao candidato ao emprego, uma vez que a finalidade que motivou ao tratamento dos dados pessoais não chega a se verificar, isto é, a celebração do contrato de trabalho não ocorre, concluímos que a generalidade dos dados fornecidos por este ao responsável pelo tratamento podem sempre ser apagados, ou seja, o candidato ao emprego terá sempre na sua disposição o exercício do direito ao esquecimento relativamente a todo e qualquer dado ou informação pessoal e profissional que tenha facultado com o único objetivo de preencher o posto de trabalho.

Assim, o empregador não terá qualquer fundamento jurídico para, sem o consentimento do candidato ao emprego, continuar o tratamento dos referidos dados, ainda mais quando este já o tenha solicitado o referido apagamento. Pelo que, deverá o empregador, enquanto responsável pelo tratamento, proceder ao apagamento dos dados pessoais do candidato ao emprego, enquanto titular dos dados, sem demora injustificada, uma vez que estes dados deixaram de ser necessários para a finalidade que motivou a sua recolha e tratamento.

Em outras palavras, podemos dizer que o candidato ao emprego goza de um pleno direito ao esquecimento.

6.4.1.2.O trabalhador e o direito ao esquecimento

Pela aceção do art.º11.º do CT, podemos depreender que é trabalhador, uma pessoa singular que se obriga, mediante retribuição, a prestar a sua atividade a outra ou outras pessoas, no âmbito de organização e sob autoridade desta. Embora existam outras modalidades jurídicas de prestação de trabalho, para o presente estudo, não revelam especial importância.

O vínculo jurídico entre o trabalho e o empregador é efetuado com a celebração do contrato de trabalho. Desta forma, para o cumprimento do referido contrato, ou seja, cumprimento dos deveres e o exercício dos direitos previstos no contrato de trabalho para ambas partes, é inevitável que o trabalhador disponibilize determinados tipos de dados pessoais ao empregador, para que este proceda do devido tratamento. No entanto, diferentemente do acima referido, quanto ao candidato ao emprego, existem dados a que o trabalhador está obrigado, por lei, e outros que está obrigado a fornecer por imposição da organização a que se insere, esses não são

apenas dados pessoais gerais sobre a vida pessoal e profissional deste. Porém, as restrições quanto às informações que o empregador não pode exigir do candidato ao emprego previstas no art.º17.º, n.º1, aplicam-se, nos mesmos termos ao trabalhador.

Ao trabalhador, além dos dados pessoais de carácter mais gerais, uma vez que já está inserido numa relação laboral, diversas outros tipos de dados pessoais lhe são solicitados, nomeadamente, dados referentes a contas bancárias, geralmente para o efeito de processamento salarial e dados biométricos, estes, nos termos do artigo 18.º, n.º 1 do CT, apenas podem ser tratados pelo empregador após notificação à CNPD, complementarmente, o tratamento de dados biométricos deve basear-se em métodos cientificamente reconhecidos e deve estar sujeito a requisitos de segurança e proporcionalidade rigorosos⁷³. Deste modo, para nós, é evidente que o nível de responsabilidade no tratamento destes dados pessoais por parte do empregador é acrescido, razão pela qual, a tutela dos direitos do trabalhador para efeitos da sua segurança jurídica no decorrer da relação contratual, também será acrescida, para que não exista margem para violação dos seus direitos, e nem para o incumprimento dos seus deveres.

Portanto, para que o trabalhador possa exercer o direito ao esquecimento, é necessário que seja feita uma análise casuística dos dados pessoais ou da informação que o trabalhador pretenda ver esquecida. Isto porque, estando o trabalhador vinculado há um contrato de trabalho, existem dados que inevitavelmente têm de ser tratados pelo empregador para a subsistência do contrato e da relação jurídica subjacente ao mesmo.

Ora, o Conselho da Europa já se pronunciou relativamente à esta questão. Assim, conforme recomendação⁷⁴ desta organização, o trabalhador deve ter o direito de obter a retificação, o bloqueio ou o apagamento dos dados pessoais que lhe digam respeito, se estes forem inexatos e/ou se o seu tratamento for contrário à lei ou aos princípios enunciados naquela recomendação. No entanto, esta norma pode ser derogada por previsão legal e desde que a derrogação constitua uma medida necessária numa sociedade democrática, para proteger a segurança do Estado, a segurança pública, interesses económicos e financeiros importantes do Estado ou a prevenção

⁷³ Conselho da Europa, *Recomendação CM/Rec (2015) 5 do Comité de Ministros aos Estados Membros sobre o tratamento de dados pessoais no contexto laboral*, ponto 18.2 (1 de abril de 2015, disponível em:

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

⁷⁴ Conselho da Europa, *Recomendação CM/Rec (2015) 5 do Comité de Ministros aos Estados Membros sobre o tratamento de dados pessoais no contexto laboral*, ponto 11.2 (1 de abril de 2015, disponível em:

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

e repressão de infrações penais, a proteção da pessoa em causa ou os direitos da pessoa em causa ou os direitos e liberdades de terceiros.

Em todo o caso, para o trabalhador fazer uso do exercício do direito ao esquecimento, poderá sempre recorrer ao artigo 17.º do RGPD, desde que exista fundamento legítimo previsto numa das alíneas do n.º 1 do mesmo artigo. Contudo, como já referido algumas vezes, este direito não é absoluto, razão pela qual, o trabalhador não o poderá exercer a todo o momento e sobre todos e quaisquer dados pessoais ou informações que o empregador dispõe, caso contrário o contrato de trabalho perderia a sua eficácia.

Posto isto, somos de concluir que, o trabalhador, na vigência do contrato de trabalho, goza de um direito ao esquecimento restrito, isto é, não poderá exercer o direito sobre todos e quaisquer dados pessoais ou informações que lhe digam respeito, sob pena de esvaziar o efeito útil do contrato de trabalho. Informações referentes aos seus dados de identificação, por exemplo, são fundamentais para a subsistência do contrato de trabalho.

Por seu turno, se estiverem em causas informações e dados pessoais que não têm relevância para a subsistência do contrato de trabalho, mesmo que o trabalhador tenha consentido o seu tratamento, este pode solicitar que o empregador elimine essa informação ou dado pessoal, nos termos e para os efeitos do previsto no art.º17.º, n.º1, al. b) do RGPD. Por fim, o mesmo se aplicará aos dados pessoais ou informações do trabalhador que sejam inexatas, bem como situações que tenham ocorrido no local do trabalho e que o trabalhador tenha sido envolvido e que se trate de uma situação que poderá prejudicar a honra, bom nome, ou ferir algum direito de personalidade, se tal acontecimento não tiver relevância no contexto da prestação do trabalho em causa, o trabalhador poderá exigir que tal facto seja esquecido.

6.4.1.3.O ex-trabalhador e o direito ao esquecimento

Segundo António Monteiro Fernandes⁷⁵, muitos dos mais delicados e complexos problemas surgidos na prática das relações de trabalho respeitam à desvinculação das partes. Esta desvinculação ocorre maioritariamente através da cessação do contrato.

De acordo com o autor, a cessação do contrato tem consequências bastante mais consideráveis na esfera do trabalhador do que na do empregador. Isto porque, para o trabalhador, o vínculo laboral é o suporte de um estatuto económico, social e profissional, uma vez que o trabalhador empenha nele a sua força de trabalho (através da oferta da sua disponibilidade) e condiciona por ele, em regra, toda a sua esfera económica e mesmo o seu estatuto social. Assim, a cessação do contrato significará, para o trabalhador, o termo de uma posição global a que se ligam necessidades fundamentais. Por seu turno, para o empregador, a cessação do contrato de trabalho, quando não decorrente de sanção disciplinar, representará, normalmente, a abertura de uma vaga na organização da empresa, eventualmente a perda de um trabalhador muito qualificado, ou seja, um facto com significado económico-organizacional, mas não um evento com incidência na sua vida pessoal⁷⁶.

Ora, no que respeita à proteção de dados pessoais não podia ser diferente, pelo que, a cessação do contrato de trabalho, ou seja, a desvinculação da relação laboral, terá, igualmente, consequências mais consideráveis na esfera do trabalhador enquanto titular dos dados pessoais, do que na esfera do empregador, enquanto responsável pelo tratamento.

Desta forma, mesmo após a cessação do contrato de trabalho, “*O exercício do direito ao esquecimento pode ser considerado como um desmembramento do direito à reserva de intimidade privada do trabalhador, como se revelou de forma sintomática no caso de uma apresentadora brasileira que, no passado, fez um determinado filme do qual mais tarde se arrependeu e que ela não mais deseja que seja exibido ou rememorado por lhe causar prejuízos profissionais e transtornos pessoais*”⁷⁷. Pelo que, após a cessação do contrato de trabalho é possível ao trabalhador o exercício deste direito, porém, apenas em determinadas circunstâncias e desde que não existam interesses legítimos prevalecentes que justifiquem manutenção do

⁷⁵ Monteiro Fernandes, António (2009), *Direito do trabalho*, p. 547.

⁷⁶ Monteiro Fernandes, António (2009), *Direito do trabalho*, p. 548

⁷⁷ Acórdão do Tribunal da Relação de Lisboa, processo n.º 12234/21.0T8LSB.L1-7, Relator, Luís Filipe Pires de Sousa, disponível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6b57c49941d5779f802589aa0049be2a?OpenDocument>

tratamento dos dados. Consequentemente, os dados pessoais do trabalhador não devem ser conservados pelos empregadores por um período superior ao justificado pelas finalidades do contrato de trabalho referidos no princípio 2 das recomendações do conselho da europa para esta questão⁷⁸ ou ao exigido pelos interesses do trabalhador ou antigo trabalhador⁷⁹.

Quando ocorre a cessação do contrato de trabalho, a finalidade que motivou a recolha e tratamento dos dados pessoais deixa de existir, em consequência disso, por força do art.º17.º, n.º1, al. a) do RGPD, o titular dos dados tem o direito de exigir ao responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este a obrigação de os pagar, sem demora injustificada. Todavia, como vimos, os efeitos da extinção da relação laboral não são imediatos, ou seja, mesmo com a cessação do contrato de trabalho, existem direitos e deveres a que as partes estão vinculadas por força do referido contrato, por esta razão, em relação a determinadas informações ou dados pessoais, o trabalhador não poderá exercer este direito de forma imediata, pensemos, por exemplo, nos dados referentes à conta bancária do trabalhador, que o empregador deverá manter até o cumprimento integral de todas as obrigações retributivas que tem para com o trabalhador, acertos salariais, subsídios de férias, natal, etc.

O CT prevê determinadas situações que pressupõe a manutenção dos dados do trabalhador para que o empregador possa exercer alguns direitos, nomeadamente, no âmbito da impugnação da resolução do contrato trabalho. Nos termos do artigo 398.º, n.º2 do CT, a ação judicial destinada a averiguar a ilicitude da resolução do contrato de trabalho deve ser intentada no prazo de um ano a contar da data da resolução. Desta norma depreende-se que o trabalhador que tiver resolvido o contrato não poderá, imediatamente a seguir a essa resolução, solicitar ao empregador o apagamento de determinados dados pessoais e informações que lhe digam respeito. Nesta situação, será legítimo ao empregador escusar-se do cumprimento dessa obrigação com o fundamento de estar em tempo para uma possível ação judicial destinada a averiguar a ilicitude da resolução do contrato. Nestes casos, por exemplo, o apagamento dos

⁷⁸ “As “finalidades do trabalho” dizem respeito às relações entre empregadores e trabalhadores que se prendem com o recrutamento, a execução do contrato de trabalho, a gestão, incluindo o cumprimento das obrigações previstas na lei ou em convenções colectivas, bem como o planeamento e a gestão eficaz de uma organização e a cessação da relação de trabalho. As consequências da relação contratual podem prolongar-se para além do período de vigência do contrato de trabalho;”

⁷⁹ Conselho da Europa, *Recomendação CM/Rec (2015) 5 do Comité de Ministros aos Estados Membros sobre o tratamento de dados pessoais no contexto laboral*, ponto 13.1, 1 de abril de 2015, disponível em:

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

dados apenas poderá ocorrer decorrido este prazo e caso o empregador não faça uso desta faculdade que lhe é conferida.

Por tudo o que foi exposto, somos de concluir que, com a cessação do contrato de trabalho e desvinculação da relação laboral, o ex-trabalhador goza de um direito ao esquecimento limitado ao tipo de informação ou dados pessoais, ao cumprimento de obrigações decorrentes do termo da relação jurídica e aos prazos legais do exercício de direitos e interesses legalmente protegidos a cada uma das partes com a extinção da relação laboral.

7. O contributo do processo C-131/12, Google Spain SL, Google Inc. v. Agência Espanhola de Proteção de Dados, Mario Costeja González, 13 de maio de 2014, em síntese

O avanço na matéria de proteção de dados pessoais e, especialmente, no que diz respeito ao direito ao esquecimento, teve um grande contributo da jurisprudência. Alguns são os casos jurisprudências que levaram a que a proteção de dados e o direito ao esquecimento tivessem hoje a relevância que têm, tanto a nível nacional, como a nível europeu ou mesmo internacional.

Um dos casos mais conhecidos e que fez com que esta matéria fosse mais discutida é o caso abordado no Acórdão do Tribunal de Justiça, de 13 de maio de 2014, no processo C-131/12, que teve como objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º do TFUE⁸⁰, pela Audiência Nacional (Espanha), por decisão de 27 de fevereiro de 2012, que deu entrada no Tribunal de Justiça em 9 de março de 2012, no processo Google Spain SL, Google Inc. contra Agência Espanhola de Proteção de Dados (AEPD), Mario Costeja González⁸¹.

No caso em questão, “M. Costeja González, de nacionalidade espanhola e domiciliado em Espanha, apresentou à AEPD⁸² uma reclamação contra La Vanguardia Ediciones SL, que publica um jornal de grande triagem, designadamente na Cataluna (Espanha) e contra a Google Spain e a Google Spain. Esta reclamação baseava-se no facto de que, quando um internauta inseria o nome de M. Costeja González no motor de busca do grupo Google (a seguir «Google Search»), obtinha ligações a duas páginas do jornal da La Vanguardia de, respetivamente, 19 de janeiro e 9 de março de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome de M. Costeja González”.

Com esta reclamação, “M. Costeja González pedia, por um lado, que se ordenasse à La Vanguardia que suprimisse ou alterasse as referidas páginas, para que os seus dados pessoais deixassem de aparecer, ou que utilizasse determinadas ferramentas disponibilizadas pelos motores de busca para proteger esses dados. Por outro lado, pedia que se ordenasse à Google

⁸⁰ Referente à competência do Tribunal de Justiça da União Europeia para decisões a título prejudicial.

⁸¹ Acórdão disponível em <https://curia.europa.eu/juris/document/document.jsf?jsessionid=0FE8D3363499BB3078B4C3365E8C6DAA?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=589715>.

⁸² Agência Espanhola de Proteção de Dados.

Spain ou à Google Inc. que suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nas ligações da La Vanguardia. Neste contexto, M. Costeja González alegava que o processo de arresto, de que fora objeto, tinha sido completamente resolvido há vários anos e que a referência ao mesmo carecia atualmente de pertinência”.

Desta forma, “por decisão de 30 de julho de 2010, a AEPD indeferiu a referida reclamação na parte em que dizia respeito à La Vanguardia, tendo considerado que a publicação por esta das informações em causa estava legalmente justificada, dado que tinha sido efetuada por ordem do Ministério do Trabalho e dos Assuntos Sociais e teve por finalidade publicitar ao máximo a venda em hasta pública, a fim de reunir o maior número possível de licitantes”.

Em contrapartida, “deferiu esta mesma reclamação na parte em que dizia respeito à Google Spain e à Google Inc. A este respeito, a AEPD considerou que os operadores de motores de busca estão sujeitos à legislação em matéria de proteção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação. A AEPD considerou que estava habilitada a ordenar a retirada dos dados e a interdição de aceder a determinados dados, por parte dos operadores de motores de busca, quando considere que a sua localização e a sua difusão são suscetíveis de lesar o direito fundamental de proteção dos dados e a dignidade das pessoas em sentido amplo, o que abrange também a simples vontade da pessoa interessada de que esses dados não sejam conhecidos por terceiros”.

Por conseguinte, a Google Spain e a Google Inc. interpuseram dois recursos separados da referida decisão na Audiência Nacional, que decidiu apensá-los.

Em consequência disso, a Audiência Nacional decidiu suspender a instância e submeter ao Tribunal de Justiça, entre outras, seguinte questão prejudicial:

“No que respeita ao âmbito do direito de apagamento e/ou [de] oposição em conjugação com o ‘direito a ser esquecido’: Devem os direitos ao apagamento e bloqueio dos dados, regulados no artigo 12.º, alínea b), e o direito de oposição, previsto no artigo 14.º, [primeiro parágrafo,] alínea a), da Diretiva [95/46/CE] ser interpretados no sentido de que permitem que a pessoa em causa possa dirigir-se aos motores de busca para impedir a indexação da informação referente à sua pessoa, publicada em páginas web de terceiros, com base na sua vontade de que a mesma não seja conhecida pelos internautas quando considere que lhe pode ser prejudicial ou deseje

que seja esquecida, mesmo tratando-se de uma informação publicada licitamente por terceiros?”

“Assim, o artigo 7.º da Carta garante o direito ao respeito pela vida privada, enquanto o artigo 8.º do mesmo diploma proclama expressamente o direito à proteção dos dados pessoais. Os n.ºs 2 e 3 deste último artigo precisam que esses dados devem ser objeto de um tratamento leal, para finalidades determinadas e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, que todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação e que o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Estas exigências encontram aplicação, nomeadamente, nos artigos 6.º, 7.º, 12.º, 14.º e 28.º da Diretiva 95/46”.

“O artigo 12.º, alínea a), da Diretiva 95/46 dispõe, por sua vez, que os Estados-Membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento, consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na Diretiva 95/46, nomeadamente devido ao carácter incompleto ou inexato desses dados. Dado que esta última precisão, relativa ao caso de incumprimento de algumas exigências previstas no artigo 6.º, n.º 1, alínea d), da Diretiva 95/46, reveste carácter exemplificativo e não taxativo, conclui-se que a não conformidade do tratamento, suscetível de conferir à pessoa em causa o direito garantido no artigo 12.º, alínea b), da referida diretiva, pode também decorrer do incumprimento das outras condições de licitude impostas por esta diretiva ao tratamento de dados pessoais”.

“Nos termos deste artigo 6.º e sem prejuízo das disposições específicas que os Estados-Membros possam prever para o tratamento com finalidades históricas, estatísticas ou científicas, incumbe ao responsável pelo tratamento assegurar que os dados pessoais sejam «objeto de um tratamento leal e lícito», sejam «recolhidos para finalidades determinadas, explícitas e legítimas e não sejam posteriormente tratados de forma incompatível com essas finalidades», sejam «adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente», sejam «exatos e, se necessário, atualizados» e, por último, sejam «conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente». Neste contexto, esse responsável deve tomar todas as medidas razoáveis para que os dados que não cumpram as exigências desta disposição sejam apagados ou retificados”.

Desta forma, os pedidos efetuados ao abrigo dos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46 podem ser diretamente dirigidos pela pessoa em causa ao responsável pelo tratamento, que deve então examinar devidamente se os mesmos têm razão de ser e, se for caso disso, pôr termo ao tratamento dos dados em questão. Quando o responsável pelo tratamento não dê seguimento a esses pedidos, a pessoa em causa pode submeter o assunto à autoridade de controlo ou aos tribunais, para que estes efetuem as verificações necessárias e ordenem a esse responsável a tomada de medidas precisas em conformidade.

“Tratando-se de uma situação como a que estava no processo, que diz respeito à exibição, na lista de resultados que o internauta obtém ao efetuar no Google Search uma pesquisa a partir do nome da pessoa em causa, de ligações a páginas de arquivos em linha de um jornal que contém anúncios que mencionam o nome dessa pessoa e que respeitam a uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, há que considerar que, tendo em conta o caráter sensível, para a vida privada dessa pessoa, das informações contidas nesses anúncios e o facto de a sua publicação inicial remontar há 16 anos, a pessoa em causa tem comprovadamente direito a que essas informações já não sejam associadas ao seu nome através dessa lista. Por conseguinte, na medida em que, no caso em apreço, não parece haver razões especiais que justifiquem um interesse preponderante do público em ter acesso a essas informações no âmbito dessa pesquisa, o que, todavia, cabe ao órgão jurisdicional de reenvio verificar, a pessoa em causa pode, ao abrigo dos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46, exigir a supressão das referidas ligações dessa lista de resultados”.

Pelos fundamentos expostos, e outros, o Tribunal de Justiça (Grande Secção), declarou que:

1. “Os artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, para respeitar os direitos previstos nestas disposições e desde que as condições por elas previstas estejam efetivamente satisfeitas, o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita”.

2. “Os artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, no âmbito da apreciação das condições de aplicação destas disposições, importa designadamente examinar se a pessoa em causa tem o direito de que a informação em questão sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.º e 8.º da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão”.

Ora, com este processo, a matéria de proteção de dados e em especial, a matéria do direito ao esquecimento começou a ser estudada de forma mais intensa. Facto que posteriormente deu origem à inserção, no RGPD, de uma norma expressa que consagra o direito a apagamento dos dados ou direito a ser esquecido.

Para além disso, este processo também foi muito importante na medida em que contribuiu na delimitação do percurso a percorrer, quer pelo responsável pelo tratamento, quer pelas autoridades de controlo, tribunais, nacionais e internacionais para a determinação e averiguação das condições de aplicabilidade do direito ao esquecimento subsumido ao caso concreto. Isto porque, pelos excertos acima retiradas do processo, conseguimos delimitar alguns critérios e passos fundamentais na aplicação e verificação dos requisitos para o exercício efetivo do direito ao esquecimento. Dito de outro modo, podemos concluir que este processo constitui um guia prático para as decisões sobre a aplicabilidade ou não deste direito, tal como tem acontecido nacional e internacionalmente, na medida em que as decisões dos tribunais mencionam quase sempre este processo quando está em causa a apreciação pelos tribunais do exercício do direito ao esquecimento por parte do titular dos dados.

8. Os passos para o exercício do direito ao esquecimento

Da análise legislativa, doutrinária e jurisprudencial supra, bem como da análise do processo acima descrito, retiramos que, em termos gerais, o percurso a adotar para a determinação da existência ou não do direito a exercer o direito ao esquecimento será, em termos gerais e ao nosso entender, o seguinte:

1. Compreender se os dados pessoais ou informação em causa, a que se requer o direito ao esquecimento pode ser classificada como “dados pessoais”;
2. Identificar o responsável pelo tratamento, bem como identificar da atividade descrita como “tratamento de dados pessoais”;
3. Identificar se o titular dos dados tem direito a ser esquecido nos termos do n.º 1 do artigo 17.º do RGPD. Ou seja, se o seu pedido pode ser enquadrado nalguma das alíneas desse preceito;
4. Identificar se está em causa alguma das exceções previstas no n.º 3 do artigo 17.º do RGPD;
5. Solicitar o apagamento junto do responsável pelo tratamento.

No que diz respeito às instâncias a percorrer, concluímos que o titular dos dados que queira exercer o direito ao esquecimento deverá, em primeira instância, solicitar o apagamento junto do responsável pelo tratamento. Embora a lei preveja a possibilidade de recurso direto para as autoridade de controlo, em bom rigor, o titular dos dados deverá, a nosso ver, primeiramente, solicitar junto do responsável pelo tratamento dos dados a sua intenção de exercer o direito ao esquecimento. Posteriormente e, caso o responsável pelo tratamento de forma injustificada não dê razão ou não atenda à pretensão do requerente, este deverá recorrer às autoridades de controlo nacionais, no caso português, a Comissão Nacional de Proteção de Dados, que por sua vez, tem meios disponíveis para exigir do responsável pelo tratamento o referido apagamento de dados, ou para remeter a questão a instâncias superiores, se assim o entender. Por outro lado, ainda está à disposição do titular dos dados os tribunais nacionais e em última instância o Tribunal de Justiça da União Europeia.

Desta forma, e no âmbito do presente estudo, foi efetuado o seguinte pedido de esclarecimento junto da CNPD: *gostaria de solicitar a vossa colaboração no sentido de perceber até que ponto o direito ao esquecimento previsto no artigo 17.º do RGPD tem aplicabilidade prática em Portugal em especial no âmbito laboral e se existem processos nesse sentido.*

A CNPD respondeu ao pedido com a seguinte informação:

No seguimento da sua exposição informamos que esta Comissão não tem bases de dados que permitam verificar a questão colocada. As Deliberações desta Comissão são publicadas no nosso site em <https://www.cnpd.pt/deciso/es/deliberacoes/>.

Ora, consultado o site da CNPD, nas suas deliberações, não foram encontradas nenhuma deliberação que vão no sentido da pesquisa do presente trabalho. O que nos leva a concluir que os pedidos no âmbito do direito ao esquecimento nas relações laborais, a existirem, são efetuados diretamente para o responsável pelo tratamento e este dá o devido seguimento sem que seja necessária a intervenção da autoridade de controlo. Não obstante os casos dos pedidos efetuados diretamente no âmbito de processos judiciais e a possibilidade do recurso ao TJUE.

9. Conclusão

A presente dissertação, elaborada como requisito parcial para a obtenção do grau de Mestre em Direito das Empresas e do Trabalho, com especialização no direito do trabalho, teve como objeto de estudo o tema, *Da proteção de dados pessoais ao direito ao esquecimento do trabalhador à luz do RGPD*. Desta forma, foi feita a análise das principais questões em volta do tema, através de análise legislativa, doutrinária, jurisprudencial, incluindo o estudo do direito comparado.

Isto posto, com a elaboração do presente estudo, conseguimos chegar, entre outras, às seguintes conclusões:

1. A proteção de dados pessoais surgiu pela necessidade de proteção do direito da privacidade dos cidadãos. Direito este já vinha consagrado em instrumentos como a Declaração Universal dos Direitos Humanos de 1948, o Pacto Internacional sobre os Direitos Civis e Políticos, a Carta dos Direitos Fundamentais da União Europeia, Convenção Europeia dos Direitos do Homem, Convenção n.º 108.º do Conselho da Europa de 1981, a Diretiva 95/46/CE do parlamento Europeu e do Conselho e o Regulamento Geral sobre a Proteção de Dados.
2. Apesar de não ser recente, o direito da proteção de dados pessoais tem vindo a ganhar destaque a nível nacional, europeu e internacional. Consequentemente, a legislação sobre esta matéria tem sido atualizada por forma a acompanhar os avanços tecnológicos que exigem que a proteção conferida aos titulares dos dados pessoais acompanhe os efeitos dos avanços da tecnologia e do fenómeno da globalização.
3. A proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais é um direito fundamental, apesar disso, o direito à proteção de dados não é absoluto, pelo que, deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.
4. O RGPD prevê a possibilidade de os Estados-Membros poderem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e

organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

5. O art.º17.º, n.º1 do CT prevê determinados tipos de informações em que o empregador não pode exigir ao candidato ao emprego ou do trabalhador, nomeadamente, informações sobre a vida privada, salvo se estas forem estritamente necessárias e relevantes para avaliar a aptidão no que respeita à execução do trabalho, dados relativos à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza de atividade profissional o justifiquem, por forma a proteger a intimidade e a vida privada destes.
6. O direito ao esquecimento teve grande contributo da jurisprudência, especialmente do processo C-131/12, Google Spain SL, Google Inc. v. Agência Espanhola de Proteção de Dados, Mario Costeja González, 13 de maio de 2014, ainda no âmbito da Diretiva 95/46/CE do parlamento Europeu e do Conselho, onde foi preciso a conciliação de dois direitos para se chegar à formulação do direito ao esquecimento, especificamente, o direito ao acesso e o direito de oposição da pessoa em causa.
7. A relevância do direito ao esquecimento no direito do trabalho pode ser subsumida nas três fases da relação laboral, isto é, na fase pré-contratual, enquanto candidato a emprego, na fase contratual, enquanto trabalhador e na fase pós-contratual, enquanto ex-trabalhador. No entanto, o exercício deste direito varia consoante a fase contratual em que se encontra, bem como os tipos de dados pessoais ou informações que são objeto de tratamento.
8. Tal como a proteção de dados pessoais, direito ao esquecimento em termos gerais, não é absoluto.
9. A CNPD não tem deliberações sobre pedidos de exercício do direito ao esquecimento do trabalhador, o que nos leva a concluir que, em Portugal, ou este direito é exercido diretamente junto dos responsáveis pelo tratamento, ou não é de todo exercido.
10. Diversos esforços legislativos nesta matéria foram efetuados no sentido de acompanhar o avanço tecnológico e de conceder ao titular dos dados a proteção jurídica necessária à salvaguarda dos seus direitos, liberdades e garantias referentes ao tratamento dos seus dados pessoais. No entanto, o exercício efetivo deste direito ao esquecimento no âmbito laboral não tem tido, por enquanto, grande utilidade prática.

10. Bibliografia e Referências

10.1. Fontes normativas

Carta dos Direitos Fundamentais da União Europeia (Carta) (2000/C 364/01), *Jornal Oficial n.º C 364 de 18/12/2000*.

Código do Trabalho (CT), aprovado pela *Lei n.º 7/2009, de 12 de Fevereiro*.

Constituição da República de Moçambique.

Constituição da república portuguesa (CRP), *Diário da República n.º 86/1976, Série I de 1976-04-10*.

Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, de 27 de junho de 2014.

Convenção Europeia dos Direitos do Homem (CEDH), *Roma 05/11/1950*.

Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108), *Diário da República I-A, n.º 159, de 09/07/1993 (Resolução da Assembleia da República n.º 23/93)*.

Declaração universal dos Direitos Humanos (DUDH), *Diário da República, I Série, n.º 57/78, de 9 de Março de 1978*.

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, *Jornal Oficial n.º L 281 de 23/11/1995, p. 31–50*.

Lei de Hesse, *Hessisches Datenschutzgesetz*.

Lei Federal de proteção de dados, *Federal Data Protection Act (BDSG)* de 30 de junho de 2017, *Bundesdatenschutzgesetz*.

Lei n.º 03/2017, de 9 de janeiro, Lei das Transações Eletrónicas.

Lei n.º 121/IX/2021, de 17 de março.

Lei n.º 133/V/2001, de 22 de janeiro, que aprovou o regime jurídico geral de proteção de dados pessoais em Cabo-Verde.

Lei n.º 41/VIII/2013, de 17 de setembro.

Lei n.º 58/2019, de 8 de agosto, *Diário da República n.º 151/2019, Série I de 2019-08-08, p. 3-40*.

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

Ley Orgánica 3/2018, de 5 de dezembro, destinada à Proteção de dados pessoais e garantia dos direitos digitais.

Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), aprovado para ratificação pela Lei n.º 29/78, de 12/06, retificada mediante retificação publicada no *Diário da República n.º 153/78, de 06/07*.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, *Jornal Oficial n.º L 119, 4/05/2016, p. 1–88*.

10.2. Fontes doutrinárias e outras

Ataíde, Rui Paulo Mascarenhas (2019), “Direito ao esquecimento”, in *Cyberlaw*, Vol. 1, n.º7.

Conselho da Europa, Recomendação CM/Rec (2015) 5 do Comité de Ministros aos Estados Membros sobre o tratamento de dados pessoais no contexto laboral.

Cordeiro, A. Barreto Menezes (2020), *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, Almedina.

Grupo de trabalho do artigo 29.º para a proteção de dados, no parecer 2/2017, de 8 de junho sobre o tratamento de dados no local de trabalho.

Jeeroen. Van Den Hoven (2008), em “Information technology, privacy, and the protection of personal data”, *Information technology and moral philosophy*, Cambridge: Cambridge University.

Jerónimo, Patrícia (2015), *Lições de Direito Comparado*.

Leão, Anabela Costa; Neves, Inês; Coutinho, Juliana Ferraz (2019), *E-book: Declaração Universal dos Direitos Humanos | Convenção Europeia dos Direitos Humanos. Anotações pelos estudantes da Faculdade de Direito da Universidade do Porto*.

Monteiro Fernandes, António (2009), *Direito do trabalho*, 14ª edição, Almedina.

Studart, Ana Paula Didier & Martinez , Luciano (2019), O Direito ao Esquecimento como Direito fundamental nas relações laborais.

Suárez, Arturo Montesdeoca (2022), Tese de Doutorado, *De la protección de datos personales a la construcción de un catálogo de derechos digitales de las personas trabajadoras*, Universidade de Las Palmas de Gran Canaria.